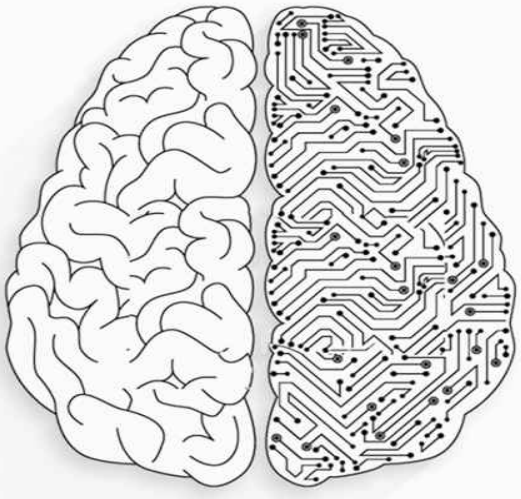
THE HUMAN MACHINE TEAM



How to Create Synergy Between Human & Artificial Intelligence That Will Revolutionize Our World

Brigadier General Y.S

THE HUMAN MACHINE TEAM

How to Create Synergy between Human & Artificial Intelligence that will Revolutionize Our World

BRIGADIER GENERAL Y.S

Producer & International Distributor
eBookPro Publishing
www.ebook-pro.com

The Human-Machine Team
Brigadier General Y.S

Contact: Yossi.human.machine@gmail.com

Contents

AN ELEVATOR SPEECH

"Can you explain the main idea of your book in 60 seconds?" My first instinct is to answer, "No! Definitely not! This is a book. I've worked on it for hundreds of hours and if the subject interests you, you have to invest at least a few hours reading and learning." Yet on second thought, in the Digital Era (DE), if you don't know how to explain a complicated issue in a few simple sentences, you cannot explain it in thousands of words and many hours of study.

Today, we are only at the threshold of the acceleration of the Digital Era. The riddle this book seeks to solve is how to lead nations and organizations in the coming years, when Artificial Intelligence (AI) is going to dramatically change the world. This book is somewhere between theory and practice and gives birth to merging ideas that are taking place in between paradigms. Since cannot imagine the future of AI in 2040 or beyond, we should prepare ourselves for the next 5-10 years when we can get ready for the distant future. A machine can use big data to generate information better than humans. However, a machine can't understand context, doesn't have feelings or ethics, and can't think "out of the box." Therefore, rather than prioritizing between humans and machines, this book is about The Human-Machine Team ("super- cognition") and about the collaboration between human intelligence and artificial intelligence. *The Human-Machine Team* will address national security challenges and threats, lead to victory in war, and serve as a growth engine for humankind. It also offers the novel idea of "FAST" (Foundations, Acceleration, and Singularity Time) as a guiding concept of how to lead nations and organizations to a successful merger of human intelligence and artificial intelligence. The final section, "Plan of Action," is a practical

program on how to fulfill these new concepts.

PREFACE

October 27, 2018, Pittsburgh. At 9:45 a.m., Robert Bowers barged into the Tree of Life - Or L'Simcha Congregation and murdered three people who were in the middle of celebrating a baby-naming ceremony. Then he went downstairs and murdered four people who were praying. Next, he ran up to the third floor, where there was an exchange of fire with police. By the time he was finally subdued, he had killed 11 people and wounded six. An hour before the attack, Bowers had posted the following on social media:

"HIAS [a group that helps refugees] likes to bring invaders in that kill our people. I can't sit by and watch my people get slaughtered. Screw your optics, I'm going in."

Now imagine that an hour before the murderous attack, a red light flashed in the synagogue with a sign that read "Beware: There is an unfamiliar cellphone in the synagogue compound." Imagine that during the few minutes Bowers was in the synagogue parking lot, a camera – equipped with facial recognition – identified Bowers, alerted police to an imminent threat, and activated an alarm inside the synagogue for people to stop him. This alarm was based on the reasoning that months prior to the attack, Bowers had blamed Jews for helping migrants and that he also had a license to carry firearms. Imagine that two minutes later, another emergency alarm went out to the police and to members of the synagogue, based on his last post on social media that read, "I am going in."

Bowers was not on a watch list of suspected terrorists and was not known to law enforcement. However, he definitely had the potential to be known as a potential terrorist by a team comprised of humans and AI machines that work together. Human intelligence cannot connect the dots and build the profile of a suspect like Bowers – not even 20,000 analysts with

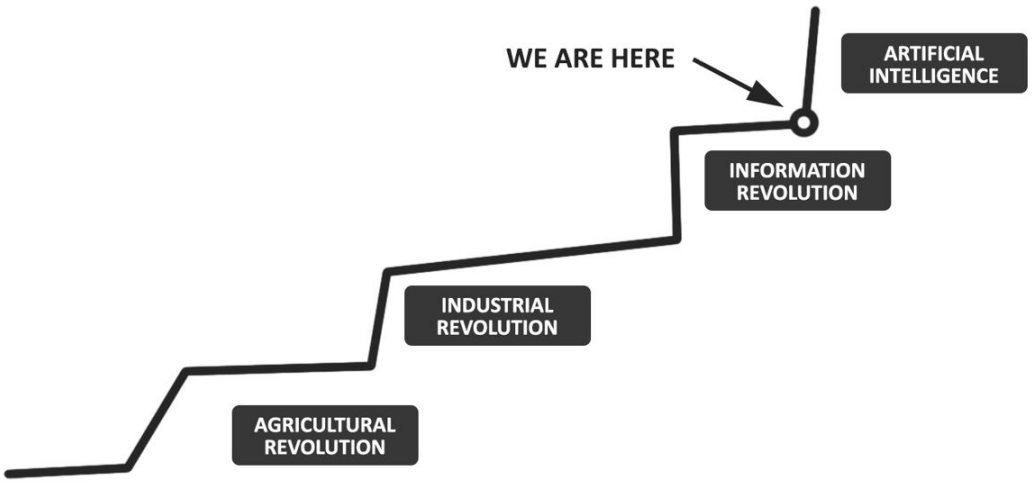
20,000,000 years of time. In addition, machine-learning by itself cannot make predictions about Bower's threat potential or decide to investigate him. However, The Human-Machine Team will lead us to a successful merger of human intelligence and artificial intelligence to address this type of threat in advance. The concept of FAST (foundations, acceleration, and singularity time) will guide us in achieving this ability.

The first step for data science is the data, and therefore we must build our data foundations in a new way that will enable this learning. In addition, we must choose specific, small capabilities and accelerate them – for example, building an AI machine to find an anomaly in a specific place and figuring out that there is a new situation that needs to be checked (like the first time that a new cellphone is in the location), and finally, to dream about the far future (singularity time) and discover ideas from the future that will also enable the current acceleration of AI. *We have no choice!* I invite you to join me on a fascinating and exciting journey to *The Human-Machine Team* , a mutual journey to discover the specific relevant steps to fulfill the potential of AI – especially, what we can do to lead our nations and organizations to a future that has already become the present, and how we should do it – starting yesterday.

INTRODUCTION

(The Responsibility of Our Generation in between Paradigms)

The viewpoint of this book is that since the development of AI, we can, and should, look at the last 40–50 years as just "foreplay" for the big changes that are about to occur in the coming years. Human cognition was the major factor that led to the development of humankind. Therefore, the ability of a machine to perform human cognition, and the ability of The Human-Machine Team to learn together and think together will create a new world. [1] This revolution creates a reality in which we can imagine a future in which people will talk about our lifetime as the beginning of a new level of *homo sapiens* (or whatever we will be called). Only decades from now – or even later – will human beings have the relevant perspective to understand these changes. In our generation, technology is not just technology that helps people; it is AI that changes people. It is AI that changes the idea of knowledge and communication. For the first time, it is not science fiction that we might be able to change our DNA. [2] We are at the threshold of the acceleration of the Digital Era Revolution. [3]



The Human-Machine Team discusses how to lead nations and organizations at this threshold of the acceleration of the DE when AI is changing the basic rules. The examples in the book are from the experience and perspective of national security, but they are also relevant for other fields, including economics, healthcare, and personal security. Every country, national establishment, and discipline can consider the book's point of view and apply it to its own field.

The book looks to follow a path that is both wide enough and narrow enough – wide enough to lead us to the future, and narrow enough to be relevant, realistic, and explain what we can and actually should do. The ideas, concepts, and practices that we build now will serve as the starting point for the next generation. Thus, a country or organization that wins the competition during this period will have the potential to define and rule the future. [4] This book is for leaders, high-ranking military officers, and high-level managers who want to lead their nations and organizations into the future, for national security officers and managers who want to put their finger on the challenges, risks, and opportunities for their organizations, and for anyone else who wants to understand AI, its

potentials, and its applications.

A Brief History of the Future

One of the common ways to describe historical divisions is by reference to major revolutions. The three major revolutions are the Agricultural Revolution, the Industrial Revolution, and the Digital Revolution. This book was written from the point of view that we are currently at the beginning of the Digital Era Revolution. From a historical perspective, every revolution, and every level in each revolution, was bigger and faster and changed more issues than the preceding one. [5]

Up until the Agricultural Revolution, people lived as nomads and in small groups. As a result, humanity began to become more than the sum of all the people together and began to live in clans and villages. During the Industrial Revolution, new technologies emerged; this revolution introduced technologies that took center stage. People invented technologies that helped them improve themselves and their lives (machines, vehicles, media, etc.). For example, it is an accepted concept to say that the United States become truly *united* only when the Industrial Revolution introduced radio and vehicles. It was then that Americans could communicate instantaneously and easily travel across the country. During the Industrial Revolution, the world organized itself with the modern concept of cities and nation-states as we know them today. Thanks to – and because of – technology, the idea of big cities and countries became a logical arrangement and turned into the main concept of living. [6]

The Digital Revolution brought with it a new, high-level paradigm. The world became a "flat world," [7] and humans were now able to communicate in ways never before imagined. The limited amount of actual data in the world developed into an explosion of information. The governments and private sectors that owned and controlled media (newspapers, radio, TV

stations, and spokespersons) were joined by public social media that was used by everyone. An extreme example of communications in the DE is the "Internet of Things" (IoT) and the "Internet of Everything" (IoE). [8] This new, high-level paradigm created a new world. [9]

Another common way to describe our time and historical divisions over the last 300 years is by the term "The Fourth Industrial Revolution." This idea was coined by Klaus Schwab, a German engineer and economist best known as the founder and executive chairman of the World Economic Forum. In his book, *The Fourth Industrial Revolution,* he describes this as a technological revolution that blurs the lines between the physical, digital, and biological spheres. From this perspective, The First Industrial Revolution began in the middle of the eighteenth century in Europe and North America, and the foremost invention that contributed to the revolution was the steam engine. It was a period when mostly agrarian, rural societies became industrial and urban. The iron and textile industries, along with the development of the steam engine, played central roles in this revolution, which also spawned the concept of big factories.

The Second Industrial Revolution, which began in the second half of the nineteenth century, lasted until World War I. It was a period of growth for pre-existing industries and the expansion of new ones, such as steel, oil, and electricity. This revolution used electric power to enable mass production. Major technological advances during this era included the telephone, light bulb, phonograph, and internal combustion engine. The Third Industrial Revolution, which began in the middle of the twentieth century, is the Digital Revolution. It refers to the advancement of technology from analog electronic and mechanical devices to the digital technology available today. Advancements during the Third Industrial Revolution include the personal computer, the internet, and communications technology.

The Fourth Industrial Revolution describes the era we live in, and builds on the Digital Revolution; it represents new ways in which technology becomes embedded within societies and even within the human body. This revolution provides increasingly faster breakthroughs in a number of fields, including robotics, artificial intelligence, nanotechnology, quantum computing, biotechnology, the Internet of Things (IoT), 3-D printing, and autonomous vehicles. Clearly, the Fourth Industrial Revolution is marked by emerging technology that continues to discover the digital code of the real world.

We do not aspire to describe an exact future, because this is obviously impossible; moreover, the future depends on us as well (as Abraham Lincoln so aptly put it, "The best way to predict the future is to create it."). Therefore, this is just a view looking forward, to think about the potential risks and potential opportunities. There are new threats, continual threats, and hybrid threats that are constantly changing due to the DE. The rules regulating the reality of our lives during this development of artificial intelligence are not the same as they were before our era. Today we live in a world in which it is difficult to hide secrets, in which data companies such as Google already have more knowledge and insight about the population than Stalin ever did about his population. This reality represents a challenge for our freedom and human rights, and opens the question about the relationship between liberty and security. Finally, it is not a fantasy to think about "Digital Countries" as a new concept of world organization.

One example of the big changes to come is how to use Gross Domestic Product (GDP). Currently, the basis for evaluating the economic situation of a country is the potential GDP, which is a way to discover the financial status of a country per year. Potential GDP is the value and productivity of the workforce. Every review and analysis of a country's economic situation begins with the workforce and its productivity. Furthermore, the potential

of the GDP, which is the basis for understanding the economic situation and the basis on which to build an economic plan, is workforce multiplied by productivity. In our lifetime, when there is machine-learning and smart robots, the potential of the workforce is infinite, and its productivity also has the potential to be infinite. [10]

The Main Characteristics of the Digital Revolution (Definitions) [11]

There are various ways to discuss and to describe our era. Information revolution, digital era, internet, network of networks, etc. – are all terms to describe the current revolution. These ideas refer to a new world when science and society will have merged. Data science, social media, artificial intelligence, neural networks, cyberspace – are all words to describe the combination of science and society that met each other, merged, and changed the course of history. *Network of networks* is a concept that describes the new world, where all people, regardless of religion, race, gender, or age, can communicate 24/7 without limits. *Cyberspace* is the domain that includes the staggering number of computers, their human users, and the networks connect them. This idea also includes the concept of a "cyber war" between computers. [12] *Internet* is the name of the platform of this network between computers. The Internet is one of the main things that accelerated big data. The *Information Revolution* (sometimes called *Information Age)* is a revolution during our lifetime, in which a lack of data transformed into today's reality of (seemingly) infinite data and information. [13]

Machine-Learning is a new potential for dealing with big data using machine power and the ability to learn and draw conclusions from big data to make predictions. This concept includes the ability to deal with big data in a way that humans could not address without machine-learning. [14] *Deep Learning* is the ability to use technology to perform activities that trace and

simulate some of the functions of the human brain through *Artificial Neural Networks,* which is the ability to convert various kinds of information to artificial neurons and then build machine- learning. [15] *Artificial intelligence* is based on the previous revolutions and innovations; it is the ability of a machine to perform (part of) human cognition and to "think" [16] and give feedback to itself. [17]

Digital – is the ability to bring our lives together using bits. It is the ability of people to represent, arrange, and process the real world through bits. The great jolt that changes our lives is the ability to take different kinds of data and digitize them into binary digits. This revolution enables the realization of new concepts. For example, when a picture can be digitized into bits, a machine has the potential to learn about the picture and compare it with other digital pictures. Digital also gave us the option to store the bits using clouds.

The *Digital Era* is a historic perspective that describes our own period, when a major revolution is taking place, one in which human beings can understand, influence, and empower life experiences by using digital bits. [18] Over the last few decades, computers have moved from being located and used in a designated room to being a part of the human body itself. They began as machines that needed large rooms, and people used the computer for its power of calculation. It continued as an essential part of peoples' desks, and integral parts of many jobs. The next step was when the computer became a smartphone in people's pockets, and smart watches on their wrists – and it is now literally becoming part of our flesh. Nowadays computers are a crucial part of peoples' lives. [19]

In the DE, we can discuss at least five different internal revolutions. The first is the ability to communicate instantaneously with all of the people (as well as many devices) all over the world. The second is the Data Revolution, which took us from the days in the past when we didn't have

enough data, to the current reality of an infinite amount of data. The third is the ability to keep all this data stored and, specifically, the ability to store it in the cloud. The infiniteness of data, and the ability to store and organize it, created the potential for the next step of Deep Learning from big data. The fourth is high-performance computing to deal with great amounts of data, and fifth is the Artificial Intelligence Revolution. [20]

"You May Say I'm a Dreamer, But I'm Not the Only One" [21]

Many books have been written about humankind in the DE. The babies who were born and raised with smartphones in their hands are not the same children that we were. For years, humans and machines have been a kind of team and have had a type of working relationship. Today, machines are different and can perform human cognitive activities. People are also not the same; therefore, the relationship between humans and machines is different and has new potentials. [22]

Artificial intelligence is a potential game changer. AI is going to address big challenges in novel and varied ways that we could not have even imagined years ago. It has the potential to improve healthcare, national security, personal security, and other vital aspects of our lives. The problems that humans didn't know how to solve in the past, AI has the potential to solve in the future. Challenges that people did not even know how to address years ago can now be examined with AI. [23]

Imagine a world in which more than 30% of the population is over age 75. Imagine a world without cancer. Imagine a world where it is difficult to hide the truth. Imagine a world in which more and more of the workforce is comprised of machines. Our culture is changing, and the machines and the robots are changing as well. Over the last few decades, the major change was to improve the efficiency of manufacturing. Pre-AI robots helped improve factories and increase productivity. Machines and robots

increasingly replace the classic workforce – which is comprised of people. The Information Revolution, data science, the capabilities of Deep Learning, machine-learning, and AI together, create a situation in which robots and machines can do things that people cannot. Machines and robots do not just do the same things greater, faster, and on a larger scale; we are talking about new things that people absolutely could not do before. It is the first time that machines have begun to perform human cognition and to "think." The actuality that machines can "think" was only realized decades after the concept was first discussed. AI has changed the rules. [24]

'In Between:' To Discover the Responsibility of Our Generation

In his book *The Structure of Scientific Revolutions* , Thomas Kuhn claims that the great revolutions of humanity arose from crises. He similarly describes the phenomenon of paradigm shifts, in which a prior paradigm gradually fills up with holes like a sieve, becoming less and less relevant, but continues to exist. At the same time, alternative paradigms develop beside it until the previous paradigm is almost eliminated and new paradigms remain. Kuhn views the interim period as a "crisis period" that usually emerges as such only in retrospect.

The ground on which we have been walking while writing this book, the streets we have wandered throughout our journey, and indeed the whole world, are all nothing but a corridor to discover "what we need to do in between the paradigms." [25] The biggest challenge is to lead our nations and organizations to fulfill these potentials. Our generation is in between revolutions and in between paradigms. Over the next few years, the merger of human and artificial intelligence will be another growth engine. The crux of our journey together with The Human-Machine Team is to discover the specific relevant steps to take our nations and organizations to the future that has already become the present. We must create our Plan of Action for

"in between," which is meant to crystallize strategic action trends so we can mitigate the risks and realize the opportunities that are hidden in the future.

I wrote this book during a year of study at the National Defense University in Washington, D.C. It was an amazing and unique "in-between" time in my career. This book is also a bit "in-between,". because it is in between theory and the realm of putting into practice, and in-between history and futurism. In between the Fourth Industrial Revolution and the next generation of revolutions. In between paradigms. In between the science of technology and leadership, and executive management. In between human intelligence and artificial intelligence. The book gives birth to ideas of merging that are taking place "in between."

Don't Ask "What Does AI Mean?" Ask "What Does AI Mean for Us?"

I have been asked thousands of times "What is AI?" or "When you say AI, what does it mean, and what does it include?" This is the main issue as a basis for this book. However, the "punchline" – and the most important question – is "What does AI mean for us, and who are we in this era?" For example, is AI a new domain for us? Is AI just a new emerging technology like other new technologies? Is AI a new weapon? AI can be an opportunity to empower the information efforts and influence military power, a new paradigm to rule the economic market, and also a new technology in the innovation system. [26] Russia, China, and the U.S. are choosing different frameworks to answer these questions. [27] Artificial intelligence has different potentials, meanings, and concepts for each organization. Therefore, the first step that every organization must take is to ask, "What is AI for our nation or organization, and how do we choose to deal with this new concept?" There are several definitions for AI, but in order to lead transformation, the challenging question is to look in the mirror and ask your organization, "What is AI for us and who are we in

this era?" [28]

The path we take for this book puts the focus on what we can and must do in the next few years. There are three main sections: The first is a discussion of the idea of synergic learning between humans and machines that creates super-cognition (The Human-Machine Team); the second discusses how to guide nations and organizations to build their FAST (foundations, accelerations, and singularity time) to realize the idea of The Human-Machine Team; and the third deals with the "Plan of Action" – that is, how to fulfill the responsibility of our generation and build the next paradigm.

---

1 Stuart J. Russell, Peter Norving. *Artificial Intelligence: A Modern Approach* (city? Pearson: 2015), 1, 30.

2 Yuval Noah Harari. *21 Lessons for the 21* st *Century* (City? Spiegel & Grau: 2018), 20-43.

3 Ajay Agrawal, Joshua Gans and Avi Goldfarb. *"Prediction Machines: The Simple Economics of Artificial Intelligence"* (City? Harvard Business Press, 2018), 7-8.

4 Yuval Noah Harari. op. cit. 73-81, 110-114.

5 Thomas W. Malone. *"Superminds"* (New York: Little, Brown and Company. 2018), 10-11, 14-15.

6 Brik Brynjolfsson, Andrew Mcafee. *The Second Machine Age* . (New York: W.W. Norton & Company, 2016), 65-66.

7 As Thomas Friedman described in his renowned book about the 21st century *"The World Is Flat."*

8 IoT means the ability of devices to communicate and interact all over the world, and IoE means the ability of both humans and devices to communicate with each other, 24/7, no matter where they are.

9 Ray Kurzweil. *The Singularity Is Near: When Humans Transcend Biology* . (city? Penguin Books: 2005), 10-21.

10 Paul R Daugherty, James H Wilson. *"Human + Machine"* (Boston: Harvard Business Review Press. 2018), 137-138.

11 This book is a journey to a new paradigm. Therefore it includes new concepts, and it is important to understand the ideas and the definitions we use in it. When we say AI, what do we mean? What is digital, and why did we decide to describe our own period as the Digital Era? If you disagree with one of our definitions, it doesn't mean you cannot be part of this journey. However, it is important to put the basic definitions as we see them "on the table" for our journey together to be more effective. We discuss all these definitions at length throughout the book. In this section, there are short, simple definitions for every complicated issue.

12 Thomas W. Malone *Superminds* (New York: Little, Brown and Company. 2018), 57.

13 Yuval Noah Harari. op. cit. xi-xix, 264-265.

14 *Prediction* is the process of filling in missing information. Prediction takes big data that you have and uses it to generate information that you don't have. Ajay Agrawal, Joshua Gans and Avi Goldfarb. *"Prediction Machines: The Simple Economics of Artificial Intelligence"* (city? Harvard Business Press,

2018), 24.
15 Thomas W. Malone. op. cit., 216-217.
16 *Think* – is an abstract word. Many books have been written about thinking. When we talk here about "the ability to think," we mean thinking as a metaphor that describes the human cognition associated with the ability to learn, to understand, to make decisions, to solve problems, etc. Another common way to describe "think" is the ability to absorb information from the environment, process the information, and reorganize the information based on human cognition.
17 Ajay Agrawal, Joshua Gans and Avi Goldfarb. op. cit., 172-173.
18 Ajay Agrawal, Joshua Gans and Avi Goldfarb. op. cit., 7-20.
19 Ray Kurzweil. op. cit., 300-306.
20 Thomas W. Malone. op. cit., 8-16.
21 The Beatles. During our year in the U.S., this amazing song became a favorite of my children.
22 Yuval Noah Harari. op. cit., xi-xi
23 Paul R. Daugherty, James H. Wilson, op. cit., 208-211.
24 Paul R. Daugherty, James H. Wilson, op. cit., 72-74, 82.
25 Paraphrased from S. Y. Agnon, well-known Israeli author.
26 Congressional Research Service on *"Artificial Intelligence and National Security"* (April, 2018), 4-8, 17-23.
27 Historically, innovations had different meanings. Nuclear weapons were a new concept of weapons that led to a new pathway to be a superpower. Digitization enables a new era and a new high-level paradigm that created a few revolutions. Cyber has become a new fighting domain. 3-D printing is a new, emerging technology to improve traditional capabilities.
28 2018 DoD Artificial Intelligence Strategy: *Harnessing AI to Advance Our Security and Prosperity* (February, 2019), 14.

PART 1

The Human-Machine Team

CHAPTER 1

Humans or Machines? Narrow AI or General AI?

When We Say "Artificial intelligence," What Do We Mean? [29]

Artificial intelligence is the ability to perform human cognition and to "think." This ability refers to the automation of activities that perform functions that require intelligence when performed by people. A I is the reality when a machine can absorb information from the environment, process it, and reorganize it. To "think" means that a machine can use this reorganized information in order to draw conclusions. Artificial intelligence is the breakthrough in building "thinking machines;" it is the ability of machines to learn from experience, and their ability to infer from learning to give feedback, make assumptions, and even reach conclusions. [30]

AI does not mean that a machine can really think like a human. It is the automation of activities that we associate with human thinking, such as decision-making, problem-solving, learning, and recognizing patterns. AI is the ability, for the first time in history, when machines and computers possess their own unique ways to automate functions that for people require intelligence. [31] Therefore it is possible to imagine a machine that acts *like* it has the ability to think. [32] Humans can conceptualize this "thinking" process as human-like intelligence to think, to give feedback, and to act according to these thoughts and this knowledge. [33]

For decades, computers have had the ability of calculation. People used this calculation power to solve problems that could not be solved without computers. [34] For years, machines and robots have been designed to replace people or to replace specific human actions in order to improve productivity. In all these examples, a human had the responsibility and the

ability to think, and ultimately to act; the role of machines was just to increase the pace. [35]

What Has Changed?

What has changed (as well as what has *not* changed) is a primary question to enable us to understand the current age. What has changed in AI and what has changed in the DE are questions we need answered in order to build our strategy framework for the discussion in our era. There are people who answer these types of questions with an extremely black or white answer. For example, they reply that either "Nothing has changed, there is nothing new under the sun, and whatever will be again," or "Everything has changed, and machines are going to control humanity." The challenge is to discover the *unique context* and the relevant changes. [36]

What Has Changed in Artificial Intelligence over the Past Few Years?

Seventy years ago, Alan Turing, a British mathematician and computer scientist who broke the enigma code during WWII, asked the question "Can machines think?" Today is the first time in history that we can answer "Yes." In one sentence, what has changed is the ability to realize the idea of AI and to build systematic, autonomous machines that perform and r epresent parts of human cognition. As we discussed, people may disagree on whether machines have acted like humans since the start of the computer era. They will say that from the beginning, computers have performed a few activities and functions that require intelligence when performed by people. However, computer activities were designed to simulate human actions – but not to simulate human thinking. In addition, the activities that are associated with human thinking were basic, and the focus was to perform these basic actions faster and on a larger scale. [37]

Today, we are talking about the ability to build systematic automation that performs and represents more and more of human cognitive activities. A few examples are the ability of a machine to take a snapshot and to understand that a certain picture is of a cat; the ability of a machine to learn through big data from the past to the future; and the ability to draw conclusions from data to make predictions. All of these are just a few examples of how AI accelerates the building of systematic automation that mimics human cognitive activities. Furthermore, A I also provides the ability to perform cognitive activities that were previously impossible for human cognition to perform alone – for example, the ability of machine-learning to address hundreds and thousands of features and then draw conclusions from this big data to make predictions. This is a unique automation of human cognitive activities. [38]

What Has Changed in the DE That Enables This AI Revolution?

- Data
- Storage capacity
- High-performance computing
- In the future: Quantum [39]

A main factor that has changed is the development of the foundations for big data that enable us to use all of the data. These "data channels," which have been built over the past several years, allow us to take the idea of machine-learning and the innovation of neural networks (Deep Learning) and create the conditions to fulfill the concept of AI. In the DE we can discuss at least five different internal revolutions: communications, infinite amount of data, data storage, high- performance computing, and AI. The notion that a machine can perform human activities first appeared 70 years ago, but the conditions were not yet available to realize it. One of the first

steps toward fulfilling this dream was "Deep Learning" as a concept to build artificial neural networks that a machine can use to simulate part of human cognitive activities. Another step was the process of "machine-learning" from big data to make predictions. A revolution, which actually created the conditions for AI to break out, was the development of *the ability to use big data* .

This ability to use big data is a result of the development of the capability to save and to tag data, and then manipulate it through high-performance computing. The perception of the cloud is the most advanced current development of the ability for the maintenance and organization of data everywhere and all of the time. The power to use data stems from the unseen, yet indispensable "sewer lines" that make the big data neighborhood livable. Nowadays, we have enough data, and we can use all of the data that is stored and organized. In addition, we have the ability to manipulate and learn from it through high-performance computing; therefore, we can finally begin to fulfill the dream of AI. [40]

What Is Changing the DE?

AI is increasing and accelerating the great revolution of the DE. [41] The potential of AI to perform human cognitive activities, including those that humans cannot perform by themselves, is beginning to change the basic rules. AI has the potential to improve healthcare, national security, personal security, and many other critical areas of our lives. Problems that human beings did not know how to solve in the past, AI has the potential to solve in the future. Challenges that people did not even know how to address years ago can now be examined with AI. Therefore, we are at the threshold of the acceleration of the Digital Era Revolution. [42]

Narrow or General?

Many people are at one of the extreme positions. On the one hand, there are people who claim that "This is the end of human history. Machines are going to replace people. If AI doesn't have feelings today, it will have them tomorrow. AI is the next developmental level of evolution. In the future, *homo sapiens* will be just part of a distant history." On the other hand, there are those who insist that "Nothing has changed. We have had computers for many years. AI is just mathematics and algorithms and not really anything new." Supporters of the former talk about General AI, sometimes called Artificial General Intelligence, or AGI. This means a machine that can r eplace the entire human being. General AI refers to a notional future with an artificial intelligence system that exhibits intelligent behavior, feelings, and context, at least as advanced as a person across the full range of cognitive tasks. Supporters of the latter talk about narrow AI, which refers just to specific capabilities and not to a new reality that changes the whole system. [43]

I don't agree with either viewpoint. It is not the ability to replace the entire human being, and it is not just another algorithm. It is not about a dystopian future in which machines can control people or make strategic decisions, and it is not just about a new emerging theology. [44] Artificial intelligence is about the ability to perform human cognition similar to part of the ability to "think." [45] It is the ability to give feedback, the ability to learn, and the ability to act. [46] It is not about the overall ability to control, and not about the overall ability to understand the mental action or the process of acquiring knowledge and understanding through thought and senses. AI is also not about the ability of a machine to have feelings or exercise ethics.

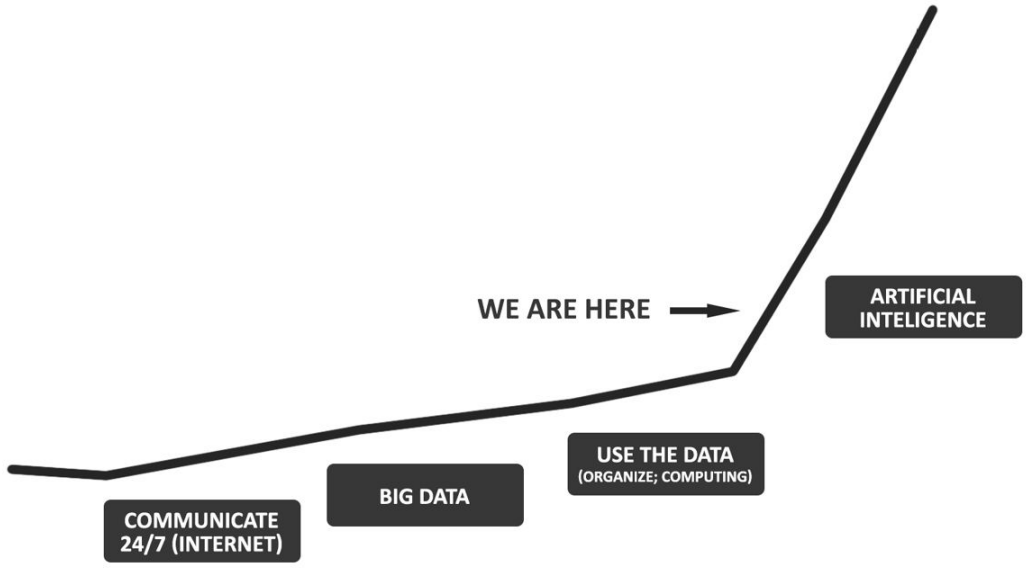
Humans or Machines?

In other words, I'm not contemplating a world out of Arnold

Schwarzenegger's *Terminator* . I'm referring to a new relationship between people and machines made possible by AI. One of the starting points for AI was the game of chess. The first time that machine-learning succeeded in beating Garry Kasparov was a tipping point in the ability of machines to "think." The human brain invented this game. For many years, computers could not beat the chess masters. It was difficult for computers to plan a few steps ahead and to know which move would be better; today, computers can beat every chess player. An even better example is when an AI machine beat the "Go" champion.[47] Compared to chess , Go is very complex and has both a larger board with more scope for play, as well as longer games. On average, there are many more alternatives to consider per move (the lower boundary on the number of legal board positions in Go has been estimated to be 2×10^{170}). In October 2015, for the first time, the AlphaGo program beat a human Go champion.[48] However, we do not yet have a machine that can invent a game like chess or Go. We still need the human brain and creativity to invent the game, and then the machine can learn the game and beat us. *Humans invented the machine that can beat them.* [49]

We can imagine a situation in the future when AI as machine-learning will build various options for games, but we will still need the human brain to make decisions about the rules. Even in unique situations that require a new strategy, such as whether to seek peace or go to war in a specific situation, we can imagine machine-learning that has the ability to give us different options about how to act. However, even then we will need the human brain to make the decisions. One human characteristic is the ability to think together with other humans. Mutual learning is one of the "magic secrets" of the development of human knowledge. Human abilities enable group thinking. AI is the ability of a machine to perform functions that are possible for people when they think, but without the ability to think together as mutual learning. AI-enabled machines can receive information

from other AI- enabled machines, but they cannot enable group thinking *between* AI machines. Therefore, I'm not talking about a fantasy world in which machines can understand complex and unique situations that have not taken place in the past. [50] Machine-learning acts as an assistant to the human. The ability to think, to give feedback and to do things that people cannot do by themselves are really changing us as human beings. Rather than prioritizing between humans and machines, I'm talking about The Human-Machine Team as "super-cognition." [51]



---

29 Brief history of AI: 1940s: The idea that machines can act with some commonalities to human behavior began to be discussed. 1950: Alan Turing, a British mathematician and computer scientist who played a central role in cracking the "Enigma Code" during World War II, published "Computing Machinery and Intelligence." His paper posed the question: "Can machines think?" This paper also discussed the potential of machines to learn from experience, much like a young child learns. 1956: John McCarthy, an American computer scientist and cognitive scientist , coined the term "Artificial Intelligence ." McCarthy put the focus on machines capable of problem-solving performance. 1969: "Shakey" is considered to be the first AI robot. It had only simple abilities, like pushing a box, but it acted with AI abilities. 1997: The year of revolution from concept to realization by IBM. The company built "Deep Blue," a computer with logic that beat Kasparov in chess. 2002-2010: More specific capabilities of AI slowly began to develop. 2010 – today: the "Spring of AI." These are the years of growth and the flowering of AI that is slowly becoming an inseparable part of our way of life.

30 Congressional Research Service. *"Artificial Intelligence and National Security"* (April, 2018), 1-4.

31 Images of the Development of AI, from left to right: Turing, John McCarthy, and the computer that beat Kasparov.

32 The idea that connected artificial intelligence to what? and created the metaphor that AI is "to think" (I think you mean that AI "thinks") first appeared in 1950, even before the term "artificial intelligence " had been coined. Alan Turing, a British mathematician and computer scientist , asked: "Can machines think?" Turing is widely considered to be a father of theoretical computer science and AI (see more on this topic later in this chapter (WHERE is this? And which chapter are you talking about?) under the heading "Brief History of AI"). Russell and Norvig, in their book on AI *Artificial Intelligence: A Modern Approach,* also address this idea with one of their definitions of AI: "systems that think like humans." "Thinking" is an abstract word. Many books have been written about it. *When we talk here about "the ability to think ," we mean thinking as a metaphor that describes the automation of activities that we associate with human thinking (decision-making , problem-solving, learning, etc.).*

33 There are various books, articles, and lectures that have tried to provide a single definition of Artificial Intelligence. Some of them define it as related to the new capabilities it brought to the world, such as the "smart house." Others define it using the image of human behavior. There are articles that focus on the potential for new conclusions and new solutions. A book on the basics of AI, *Artificial Intelligence: A Modern Approach,* written by Stuart Russell and Peter Norvig, uses the following taxonomy: (1) systems that think like humans; (2) systems that act like humans; (3) systems that think rationally; and (4) systems that act rationally. Their book is, among other things, a source of inspiration and authority for a paper published in October, 2016, by the Executive Office of the President National Science and Technology Council Committee on Technology, on "Preparing for the Future of Artificial Intelligence."

34 A good example of how people used this calculation power to solve problems that could not be solved without computers is the cracking of the Enigma Code during World War II. Enigma machines were a series of electro-mechanical rotor cipher machines mainly developed and used in the early to mid-twentieth century to protect commercial, diplomatic, and military communication. Enigma was invented by the German engineer Arthur Scherbius at the end of World War I . Early models were used commercially beginning in the early 1920s and adopted (or adapted?) by military and government services of several countries, most notably Nazi Germany , before and during World War II . Several different Enigma models were produced, but the German military models, having a plugboard, were the most complex. Cryptanalysis, using the Enigma-ciphering system, enabled the Western Allies in World War II to read substantial amounts of radio communications of the Axis Powers that had been encrypted using Enigma machines . This yielded military intelligence , which along with intelligence from other decrypted Axis radio and teleprinter transmissions, was given the codename "Ultra ." The Ultra intelligence was considered by Western Supreme Allied Commander Dwight D. Eisenhower to have been a decisive factor in the Allies' victory.

35 Stuart J. Russell, Peter Norving. op. cit. 16-27.

36 Yuval Noah Harari. op. cit. xviii-xix.

37 Thomas W Malone. op. cit. 14-16.

38 Stuart J. Russell, Peter Norving. op. cit. 30, 59.

39 In this book, I decided not to discuss the notion of quantum because it is not yet a fully developed, usable capability. It has the potential to be the biggest innovation of the future, but this book deals with the reality of the present and what we can and need to do, beginning yesterday.

40 Stuart J. Russell, Peter Norving. op. cit. 27-28, 30-31.

41 Lt.-Col. Ts, Intelligence in Theory and in Practice. "*Big Data and Intelligence*" (a Journal on Intelligence Methodology, October 2018), 24-27.
42 Yuval Noah Harari. op. cit. 3-18.
43 Executive Office of the President National Science and Technology Council Committee on Technology on " Preparing for the Future of Artificial Intelligence" (October, 2016, pp. 7-11).
44 ibid.
45 Thomas W. Malone. op. cit., 77-82.
46 Ajay Agrawal, Joshua Gans and Avi Goldfarb. op. cit., 43, 46.
47 Go is an abstract strategy board game for two players in which the aim is to surround more territory than the opponent. The game was invented in China more than 2,500 years ago and is believed to be the oldest continuously played board game.
48 In October 2015, the Google DeepMind program AlphaGo beat Fan Hui , the European Go champion, five out of five times in tournament conditions. In March 2016, AlphaGo beat Lee Sedol in three of five matches. In May 2017, AlphaGo beat Ke Jie , who at the time was ranked No. 1 in the world, in a three-game match during the Future of Go Summit .
49 Joon Ian Wong, Nikhil Sonnad. "Google's AI Won the Game Go by Defying Millennia of Basic Human Instinct" on March 25, 2016. https:// qz.com/639952/googles-ai-won-the-game-go-by-defying-millennia-of-basic-human-instinct/
50 Ray Kurzweil. op. cit., 260-262.
51 Ajay Agrawal, Joshua Gans and Avi Goldfarb. op. cit., 53-65; Thomas W. Malone. op. cit., 239-241.

CH APTER 2

“Havruta:” Synergetic Learning between Humans and Machines (Super-cognition)

We cannot imagine the future of AI in 2040 or beyond. [52] Therefore, today we are discussing the practical concept of “team.” The Human-Machine Team refers to the synergetic learning between humans and machines that creates “super-cognition.” [53] A machine can use big data to generate information better than humans can. Humans can understand context, and have feelings and ethics. A machine can take the information we have (often called “data”) and use it to generate information we don’t have, and humans can think “out of the box.” Therefore, we are talking about the collaboration between human intelligence and artificial intelligence, and about The Human-Machine Team. [54]

Synergetic learning is the new, systematic, mutual process of a human and a machine as a learning team. For many years, humans and machines have acted as a team to achieve goals that people could not achieve by themselves. An example is a pilot and a plane that act together as a team to fulfill a mission. Synergetic learning is a new potential for The Human-Machine Team in the period of artificial intelligence. It is a concept that puts the focus on the new potential in which the period of AI enables us to learn together, [55] and it allows for the understanding of issues that the human brain cannot understand or cannot address before machines had the ability to perform human cognitive activities. [56]

Learning is idea concept with a broad meaning. It is the process by which we acquire new knowledge or modify existing knowledge, behaviors, skills, values, and preferences. The “Pavlovian Response” is a well-known example of the fact that animals can also learn. However, when we discuss the deep,

unique meaning of "human learning," we mean *conscious* learning – learning as a process that leads to change. These changes occur as a result of new understandings of the environment, ourselves, other entities, and the way that all these factors interact and influence each other. In this book, the concept of learning refers to a journey for the development of new knowledge. Learning is a mental and conceptual journey of exploring new territories of understanding and characteristics of reality. Learning, here, is the ability to start a journey in which we do not know exactly where we will find ourselves at the end of the road. Furthermore, this journey also has the potential to change a few of the aspects of who we are after the experience. [57]

The ideas of "machine-learning" and "Deep Learning" both also use the word and the meaning of "learning." These ideas refer to using a machine to acquire new knowledge and new understandings. They are concepts of new capabilities for understanding issues that were not possible to understand before the creation of these new types of artificial learning. In addition, some of these new understandings were also not achievable by humans alone. Choosing to represent these concepts with the word "learning" is not accidental; "machine-learning" and "Deep Learning" are concepts that describe the ability to attain new knowledge and new understandings as a result of the DE. "Intelligence" and "learning" are ideas from the same family; therefore, Deep Learning is a basis that enables artificial intelligence. AI is a unique ability under the umbrella of machine-learning. [58]

Deep Learning

Deep Learning is using technology to perform activities that trace parts of the capabilities of the human brain. It is when machines can simulate some of the functions of the human mind by using algorithms to connect

unrelated details in order to create a congruent picture. The new technology that helped achieve this concept is the artificial neural network. The human brain works through billions of neurons and their networks of connections; Deep Learning builds similar capabilities with an artificial neural network. [59] In fact, Deep Learning is an artificial neural network that brings new potential to trace part of the human brain. [60]

The last 10 years represent the "spring" of Deep Learning. The concept of an artificial neural network plus infinite data, along with the ability to deal with billions of details with a strong machine made it possible to trace numerous activities of the human brain. [61] A well-known example of Deep Learning is facial recognition. This is the ability of a machine to learn, through a neural network, and recognize a human face. A machine learns the picture and chooses to represent it by using millions of data points through an artificial neural network. A computer can then learn this neural network and compare it to other neural networks; the end result is facial recognition. The ability to take a picture and replace it with digital data by using a neural network enables the machine to identify the person. [62]

Synergetic Learning

Synergetic learning is a new process of mutual learning combining human intelligence and artificial intelligence. [63] Synergetic learning represents new potentials for dealing with complex, complicated issues that were unsolved until machines began to be able to "think." [64] Imagine that soon after a machine beat Kasparov in chess, he was asked to build a human-machine team composed of himself and the computer that beat him. He could surmise that such a human-machine team would never again lose to a computer, to a human, or to another human-machine team. And do you know what? If he had suggested this idea, he would have been totally right! [65] Synergetic learning is a new potential that is based on the possibility of a

machine and a human "bouncing" data, ideas, and insights off each other, and "passing" the concepts to each other to create common insights. [66]

In order to understand the power of The Human-Machine Team, we can use the metaphor of "*havruta* ." Just before delving into the idea behind havruta, let's stop and a take a look at two other examples. The first is the development of flight. Watching birds fly was a metaphor for humans to discover the idea that flight was possible. Humans saw birds flying and dreamed of the ability to fly. Technology enabled humans to invent a plane that could fly. In addition, from several aspects, planes fly better than birds. However, without the initial metaphor of birds flying in the sky, the idea of human flight would never have come up – and the plane would never have been invented. (This is also one of the reasons that a plane is structured like a bird.) [67]

The second example is the brain as a metaphor for "thinking." Having a brain, and understanding how the brain works, helped humans ask, "Can machines think?" The understanding of the brain's neural network was a metaphor for coming up with the idea of artificial neural networks. These networks do not work like the human brain, but they help perform the capabilities of human cognition. [68]

> There is a fable from the Talmud about an event that took place almost 2,000 years ago between two men, Rabbi Yohanan and Reish Lakish, which describes the idea of "havruta." Rabbi Yohanan was the head of a yeshiva (a Jewish Talmudic college) and Reish Lakish was the head of the mafia. One day, Rabbi Yohanan saw Reish Lakish transporting big logs from one side of the river to the other. Rabbi Yohanan was amazed and told him, "Your strength should be used for learning Torah (the Jewish bible)." Reish Lakish answered, "You are too handsome, and your good looks should be for a woman." They decided to make a deal. Reish Lakish would come to study in

> the yeshiva, and Rabbi Yohanan's sister, who was even better-looking than he was, would become Reish Lakish's wife. The two men became a havruta, thinking together and studying together all the time. After a few years, Reish Lakish died and the smartest student in the yeshiva became the new havruta for Rabbi Yohanan. The two began thinking and learning together, but after a while Rabbi Yohanan declared to his new havruta, "I want to die!" In shock, the smart student turned to Rabbi Yohanan and asked, "Why? What happened?" Rabbi Yohanan explained, "For every new idea that I had and then discussed with Reish Lakish, he gave me 24 reasons that I was wrong, and then we had to think together to improve our thoughts and create new knowledge together. In your case, I give you an idea and you give me 24 reasons that I am correct, so there is no new knowledge." This fable is also the reason behind another powerful sentence from the Talmud: "Havruta or death!"

"Havruta" is a metaphor to explain this new mutual learning team comprised of a human and a machine. It is an Aramaic word meaning "friendship" or "companionship," and it is a process of sy nergetic learning between humans who learn together as a team. Havruta is synergetic learning and a major way that Jewish knowledge developed over thousands of years of studying Jewish texts in groups. It is a mutual learning process that enables humans to create new knowledge and discover new understandings. There is a famous Jewish saying that a knife can only be made sharper by another knife, and this is the concept of learning together in havruta. It is all about the knowledge that is created in the interaction between the various points of view. Havruta can also be a good metaphor to explain the idea of synergetic learning between a human and a machine. "I think; therefore I am" is a well-known statement by the philosopher Descartes.[69] The ability to think is one of the "magic secrets" of humankind,

an ability that is a base for creating our reality. Human cognition enables the discovery of new innovations. [70] Today, humanity has the potential to achieve "super-cognition" with the havruta between humans and machines.

The bottom line is that the Spring of AI brings with it a new potential for merging human intelligence and artificial intelligence. Synergetic learning enables us to address national challenges in novel, atypical ways that years ago we could not have even imagined. It also enables us to discover new national security challenges, new risks, and new opportunities. With these "lenses of synergetic learning" we can dream of these new discoveries, [71] which is why the future of national security belongs to security establishments that fulfill the conditions to bring to fruition the opportunity for synergetic learning. The unique challenge of our time is the situation of being in between paradigms. This unique reality requires us to build our nations and organizations to lead the revolution when a human and a machine can think and learn together in havruta. [72]

---

52 Executive Office of the President National Science and Technology Council Committee on Technology, op. cit., 7-8.

53 The idea of "teaming" appeared in the report by the Executive Office of the President National Science and Technology Council Committee on Technology on "Preparing for the Future of Artificial Intelligence" (October, 2016, pp. 10-11). In addition, in 2018 several articles and books were published on this concept. Two books that deeply influenced my journey are *Superminds* by Thomas W. Malone (New York: Little, Brown and Company. 2018); and *Human + Machine* by Paul R. Daugherty and James H. Wilson (Boston: Harvard Business Review Press. 2018). My advisor at the NDU, Dr. James Keagle, was the first to suggest that I organize my book under the umbrella of teaming.

54 Ajay Agrawal, Joshua Gans and Avi Goldfarb, op. cit., 65-69; Thomas W. Malone. op. cit., 198-200.

55 Thomas W. Malone. op. cit., 59-62.

56 Ajay Agrawal, Joshua Gans and Avi Goldfarb. op. cit., 65-69.

57 Thomas W. Malone op. cit., 235, 239.

58 Ajay Agrawal, Joshua Gans and Avi Goldfarb. op. cit., 13.

59 Development the Idea of Deep Learning: The concept of Deep Learning first appeared in the early 1940s and was conceived by McCullon and Pitts, two American researchers who established the basis for the science of a neural network. Twenty-five years later, the idea was abandoned since important researchers claimed that it did not work then, nor would it work in the future. The first reason cited was that computers did not have enough power to deal with these networks. The second was the claim that one artificial neuron cannot do anything, so artificial neurons linked together cannot succeed either. During the 1980s, this concept became popular again due to a new understanding that the

power of this idea is the network of billions of artificial neurons. The fact that one artificial neuron could not do anything was immaterial. Instead, the concept was what billions of neurons could do linked together as a network. It is all about the network. However, Deep Learning was still waiting for data and for computers with enough power to deal with big data.

60 Stuart J. Russell, Peter Norving. op. cit., 750.

61 Ajay Agrawal, Joshua Gans and Avi Goldfarb. op. cit., 45-47.

62 From this example we can learn the basic idea behind the neural network. The idea is to build the right network for this task (the architecture of the network) and to teach the network using thousands or even hundreds of thousands of labeled data. The network changes with time, and after the training period, you have a neural network that completes a task. The neural network then codes the picture into a ??? binary data (vector), which represents the picture from then on. In order to identify a probable picture, the neural network translates the picture to a unique vector and compares it to all the vectors in the data base. For example, the data base can be all pictures that were previously converted into vectors using this specific neural network.

63 Like 54: What does this mean? The idea of "teaming" appeared in the report by Executive Office of the President National Science and Technology Council Committee on Technology on "*Preparing for the Future of Artificial Intelligence*" (October, 2016, pp. 10-11). In addition, in 2018 several articles and books were published on this concept. Two books that deeply influenced my journey are *Superminds* by Thomas W. Malone (New York: Little, Brown and Company. 2018); and *Human + Machine* by Paul R. Daugherty and James H. Wilson (Boston: Harvard Business Review Press. 2018). My advisor at the NDU, Dr. James Keagle, was the first to suggest that I organize my book under the umbrella of teaming. Why not just write "See end note 53"?

64 Thomas W. Malone. "How Can Superminds Help Solve Our Problems?" in *Superminds* (New York: Little, Brown and Company, 2018), 246-249.

65 Kasparov and the "Deep Blue" (chess computer) played 12 games during 1996-1997. After every game, the computer team learned new concepts and new tools for the next game against Kasparov.

66 jay Agrawal, Joshua Gans and Avi Goldfarb. op. cit., 65-69, 212.

67 Stuart J. Russell and Peter Norving. op. cit., 3

68 Thomas W. Malone. op. cit., 209-214.

69 This originally appeared in French as "Je pense, donc je suis."

70 Thomas W. Malone. op. cit., 171-172.

71 Ajay Agrawal, Joshua Gans and Avi Goldfarb. op. cit., 195-205.

72 Paul R Daugherty, James H Wilson. op. cit., 207-211.

CHAPTER 3

Deep Defense

Past-Future-Present (in This Order)

Strategic challenges require a process of learning. This process is based on the past, future, and present (yes, in this order). Past – to understand the genealogy and the framework we have reached to date. Future – to discover the potential risks and opportunities for the future. Present – to crystallize strategic action trends to avoid risks and seek to fulfill the opportunities. One of the ways to think about the future is the concept of scenarios. Keens Van der Heijden, in his book *Scenarios: The Art of Strategic Conversation* , develops scenarios as alternative ways to describe options for what might happen in the future. He also discusses how to utilize these scenarios in an organizational process to impact the strategy and planning of the organization as a whole and prepare it for action. Heijden explains:

"…today's best strategy may be tomorrow's disaster … the ultimate purpose of the scenario planner is to create a more adaptable organization, which first recognizes change and more uncertainty, and second uses it creatively to its advantage." [73]

These days, security leaders are required to build scenarios for security challenges in the Digital Era. These leaders must formulate scenarios for the Artificial Intelligence Revolution as a basis for their planning processes. How can AI be a possible game changer to win a war, and what do we need to do today to prepare ourselves for the near future? [74]

Past (Experience and Challenges for National Defense)

War is the supreme test of a military organization. The primary national

security mission is to protect the country and win in war. Historically, many wars have broken out without warning; moreover, some of them began even though neither side wanted a war. However, the adversaries ended up in a difficult and bloody war, and sometimes even found themselves in a war for survival. In addition, the results of war have far-reaching implications, and the results also design the future for many years. In the complex environment of the Middle East, the meaning of a "good" or "bad" war has tremendous repercussions for all sides. In the distant past, until the end of the World War II, a victory or loss in war was usually clear-cut. The winning side conquered the territory of the loser, and everyone knew who won and who lost. In the last 80 years there have been wars that ended with clear victory, there have been wars that ended without any clear defeat, and the struggle over who won and who lost exists even until today. [75]

From the Israeli perspective, there are wars like the Six-Day War in 1967 and the Sinai Campaign in 1956, [76] in which Israel defeated its enemies and the victory was clear and sharp. Conversely, there are wars such as the Yom Kippur War (1973) when both sides are convinced – even until today – that they won. In the last 20 years, the Israeli military has concluded operations and wars with a feeling of "*hachmatza* " (Hebrew for a "missed opportunity"). For example, the 2006 Winograd Commission (the Israeli government's official commission of inquiry into the Second Lebanon War) argued in detail that the Israel Defense Forces missed an opportunity to defeat Hezbollah and achieve a decisive victory, and all the operations in Gaza over the last 15 years ended without definitive results.

Moreover, over the last few decades and since the end of the Cold War, most wars and conflicts have been asymmetric. The DE empowers this asymmetric reality. Know-how that once belonged to countries became knowledge that everyone can obtain. Since the DE, every man and woman has access to more data on their smartphones than superpowers had 50

years ago. Social media created a reality in which every person can publish whatever he or she wants. In addition, the DE globally empowers the phenomenon of "lone-wolf" terror attacks. This type of attack takes place as "terror due to inspiration." A person reads something on social media or sees a picture about something that happened and decides to go out and commit an attack. Moreover, the ability to self-publish this terror attack is another issue that helps the individual make a decision to do it. From time immemorial, there have been lone-wolf terrorists, but in the DE this phenomenon has become more and more widespread. As a result, lone-wolf terrorists are a bigger challenge for national security establishments. [77]

Another complex challenge that is growing and becoming stronger is the ability to protect countries' borders from infiltrators, terrorists, underground tunnels, drones, etc. The border wall between the U.S. and Mexico is an example of this challenge. Moreover, protecting borders is also a unique challenge during war, as evidenced by the concept of attack tunnels that Hamas built along the Gazan-Israeli border, and that Hezbollah built along the Lebanese-Israeli border.

In the last few years, Hezbollah in Lebanon has a military challenge for Israel. During the Digital Era, Hezbollah, with support from Iran, has managed to arm itself with more than one hundred thousand rockets that it can use against targets in Israel. In addition, these rockets increasingly have the capabilities of guided missiles. Hezbollah uses the civilian population in Lebanon to empower its capabilities: its fighters and rockets are located strategically among the population and they commit their acts from inside the population centers. Thus it is difficult to identify and produce targets to attack the rocket launchers effectively or use special forces to prevent Hezbollah from using the rockets. In other words, it is difficult to uncover tens of thousands of launchers that are hidden within the cities and villages, and among civilian buildings and homes. Moreover,

it is very difficult to attack the launchers without harming countless innocent civilians. For example, in the Second Lebanon War in 2006, more than 4,000 rockets were fired by Hezbollah into Israel over a period of 33 days. For the next war, the threat has grown dramatically. Hezbollah plans to fire thousands of rockets against Israel every day, including guided missiles against strategic assets in the heart of the country. Preventing Hezbollah from effectively using these rockets and missiles is an extremely important undertaking. The bottom line is that over the last few decades, and specifically during the last few years, Israel finds more and more defense challenges for which our traditional abilities and strengths will not be able to completely defeat the enemy. Therefore, asymmetric conflicts have concluded without clear victories.

Future (from the AI Perspective)

In 2040, the national security organizations will be more different than similar to their structure today. They are going to be so different that we cannot even describe what the big issues and top priorities will be. In addition, we cannot even imagine the future structure of these organizations. Infinite data will be organized in such a way that everyone will be able to use it. A few significant, traditional, intelligence positions, such as audio-lingual analysts and aerial-image analysts, which today require thousands of analysts, will almost disappear and be replaced by AI machines. Big data will be the key to finding and understanding rivals and enemies. Data from hundreds of thousands of drones will be part of the basic information about everything. Classified and unclassified data will be on the same "closed-open-closed network" in a way that you can keep your secrets and at the same time enjoy the advantages of an open network. All of these are just a few examples regarding the changes that will occur by 2040. The more important changes that will take place cannot even be

imagined today; the only option is to lay the groundwork and begin the AI journey. [78]

An Example of a National Security Scenario for 2035
Hezbollah in 2035

Welcome to 2035. Hezbollah now has more than 200,000 rockets, including hundreds of guided missiles. In addition, Hezbollah has developed AI capabilities to empower its command and control system and can effectively use all of their rockets and missiles. Moreover, after Israel discovered and destroyed the underground tunnels that Hezbollah had excavated along the Israeli-Lebanese border, the organization armed itself with more than 1,000 AI drones that can penetrate Israeli territory. Hassan Nasrallah, Hezbollah's leader, is 75 years old and is looking for a historic victory against Israel. His senior commanders tell him that they can achieve this goal.

AI in 2035

The reality today (in 2035) is that AI has already increased and accelerated the DE Revolution.

This is the period when AI has begun to address challenges in novel, unusual ways that years ago we could not have imagined. Problems that humans didn't know how to solve in the past, AI has begun to solve in our lifetime. Challenges that people did not know how to address in 2020, can now be examined with AI.

"D eep Defense:" New Potentials

Deep Learning is the ability to use technology and digital capabilities to go

"deeper" and discover and understand issues that were previously "covered" and impossible to achieve. Deep defense is the ability of national establishments to use The Human-Machine Team concept to address security challenges to expose issues in new ways that were heretofore impossible. The first new potential for war is the ability to create "targets in context." The Human-Machine Team has the ability to create tens of thousands of targets before a battle begins, and to assemble thousands of new targets every day during a war. In addition, the ability to create these targets in context means that the military can attack the right targets at the right time. This means finding tens of thousands of hidden rocket launchers, understanding when they are manned with enemy fighters or unmanned, and understanding when it is possible to attack them without harming civilians. Imagine 80,000 relevant targets that are produced before combat and 1,500 new targets created every day during a war. Imagine that we have the constant ability to know whether the targets are manned with enemy fighters or unmanned. Finally, imagine a reality in which the military has the ability to strike "the right targets at the right time," destroying the target with the least possible collateral damage.

In the past, the "fire effort" that includes several capabilities to attack from afar, such as artillery from mortars and cannons, was an assistive effort in war. However, over the last few decades, the fire effort has become the major effort to win in war. The air forces and the exact weapons – specifically, guided missile fire and missile elimination – have become one of the most important capabilities for victory. This is also the reason that for decades, the armed forces of the world have been trying to improve the connection between the "intelligence factory" and the "fire factory." [79] The ability to decisively win a war requires that every day during the war, you put your enemy in a situation that is worse than the situation he faced the day before. If your enemy's situation gets worse each day, he'll want to stop

the war as soon as possible. Therefore, tens of thousands of "targets in context" have the potential to achieve this. During the last several decades, the fire effort has been very important, but most of the targets were created before the war. Meanwhile, during the war many factors change quickly, and striking a specific target at a specific time becomes a special operation requiring outstanding resources. Having the capability to increase the number of targets hit day after day, and strike these targets at the exact preferred time, can force the enemy to decide to end the war as soon as possible.

Humans are the bottleneck that prevent the creation of tens of thousands of targets in context. We cannot process that much information. If we want to create 80,000 targets before the war, we need thousands of intelligence investigators who need years to work on such a mission. Furthermore, a few weeks or a few months after these targets have been identified, the military cannot possibly know whether any individual target is still relevant. The moment the war begins, many of the original targets will have changed, and it is usually difficult to confirm whether the targets are manned with enemy fighters or unmanned. Interestingly, it doesn't matter how many people you have tasked to produce targets during the war – you still cannot produce enough targets per day. There is a human bottleneck for both locating the new targets and decision-making to approve the targets. There is also the bottleneck of how to process a great amount of data. Then there is the bottleneck of connecting the "intelligence" to the "fire."

The Human-Machine Team has the potential to bring about a revolution in the possibility of creating targets in context. A team consisting of machines and investigators can blast the bottleneck wide open. Machine-learning has the potential to deal with big data, a function that a human brain cannot perform alone, but many decisions can be made together. The

Human-Machine Team is capable of learning and drawing conclusions from big data in order to make predictions, and from these predictions creating targets and also answering the question of whether the targets are relevant in real-time. [80] This potential requires organizing all the layers of information in a way that we can build a "targets machine" based on all the data and sensors in the field; moreover, this team helps monitor ethical issues. Therefore, the decisions are not "machine decisions," but rather mutual decisions that are a result of synergetic learning. [81]

The second new potential is to use The Human-Machine Team concept to understand the changing reality of the enemy during war. As Carl von Clausewitz wrote, "War is the realm of uncertainty." The big picture of a war, and the picture of every single battle, change during the war. Moreover, since the enemy does not know how its own forces will perform during the war or exactly where they will be located, it is also going to be difficult for the friendly side to find these enemy fighters and understand the big picture. Google Maps and Waze are able to provide constant, minute-by-minute big pictures of traffic and incorporate the details of every road; these apps help drivers make decisions. Within the limitations of the metaphor, The Human-Machine Team has the potential to use AI to get a snapshot ("the trees and the forest") of the enemy at every moment and in every location to help the military forces fight and defeat the enemy. This potential is based on the new intelligence capabilities in the period of AI, such as speech-to-text and data-mining, which are good examples of the new capabilities available to create a "military Waze."

Th e third new potential is to use The Human-Machine Team to be a game changer to build a "smart border" (or "smart area") to control the borders, to figure out changes along the borders, and to use drones or other robotics in these areas. The Human-Machine Team enables a new potential for using AI to build a smart area for protecting borders. The ability to

connect various bits around the borders through machine-learning can help control and protect these areas. The smart area is required to define the location, organize the relevant sensors in the context of the operational problem, and prepare the "channels" of the information in the context of that same location.

The fourth new potential is the "influence or shaping effort" in the AI period. In the DE, truth and falsehoods are mixed. The development of media, and especially social media, contributed to this shaping of reality. Today, everyone can be a kind of media station with their own cellphone. The simplicity of tweeting, posting, and texting caused the influence or shaping effort to be a relevant part of the "act of war" as well. The shaping effort also has the potential to be a main part of either a victory or a loss; in the era of The Human-Machine Team, it can be much more relevant. For example, machine-learning can help create "influence in context," which means that different audiences and different individuals will receive the relevant data by the relevant media that has the greatest chance of influencing them. (The following sections will discuss how to develop intelligence organizations to realize this idea.)

The fifth new potential is to use The Human-Machine Team to understand ourselves. The notion that "War is the realm of uncertainty" means that we also cannot know where our forces will be positioned and how they will react during the war. One of the challenges of making decisions in war is the fact that we cannot understand our own military forces. AI has the potential not to just get a snapshot of our enemy, but also to get a "smart snapshot" of our military forces in real time to use as a tool to help make decisions.

Present: How to Develop "Deep Intelligence" + Three Case Studies

Strategy is the science of what we need to do today. Therefore, in the

present we need to crystallize strategic action trends to avoid risks and seek to fulfill the opportunities. One strategy for bringing military organizations into the future is through the novel idea of The Human-Machine Team. This is a new concept that allows the utilization of AI to win a war and to achieve a strategic decision. The DE is a main factor in enabling asymmetric conflicts in which stronger and larger military forces do not necessarily have an advantage over smaller ones. The Human-Machine Team has the potential to regain the advantage.

Deep Intelligence

Intelligence and intelligence organizations are broad issues, each of which can fill an entire book of its own. There are people who used to describe the DE as an Information Revolution or the Information Age. The information that used to be "backup" for helping make decisions became the issue in and of itself. The data that used to be in the "back" has moved to the front. Therefore, intelligence in the period of AI requires a revolution to help deal with the new paradigm and to address the new risks and new opportunities. The next few years are going to be in between paradigms. [82] In this section we will try to provide a few ideas and first thoughts for the beginning of the journey to realize the revolution of intelligence in the period of AI.

A Short Background

Intelligence has existed since the dawn of history. For thousands of years, intelligence has included people who work as spies or watchmen for a leader or commander by providing him or her with information. Intelligence organizations exist today based on the way they have been designed over the last 100 years. Our intelligence organizations were

established in the period between WWI and WWII. Organizations all over the world use different functions and abilities to stay one step ahead of their enemies and rivals. There are national bodies that customarily describe this idea with the concept of "intelligence supremacy," a concept that refers to the ability to be not only one step ahead of our enemies but also a base for power policy and power activation.

One of the ways that intelligence organizations used to respond to the questions and challenges they had to address was to create specific accessibility to relevant places, attain important bits of data, and use them to piece together the "intelligence puzzle." The aim of all this activity was, and still is, to provide the intelligence picture (a clarification of reality); to point to possible future scenarios; and to offer recommendations about the ways in which this reality could be affected. [83] The dream of every intelligence officer was to be a "fly on the wall" in the mind of the intelligence object.

Intelligence organizations used to be created for various functions, including research intelligence, technological organizations (first of all for collecting data), and special forces for intelligence missions. Traditionally, intelligence bodies were based on human intelligence, technology, and operations (in this order). During the past few years there have been changes in these organizations, most of them as a result of cyberspace. The cyber domain taught us that the whole world is interconnected. This means that – at least theoretically – one can go anywhere in the global digital network. By utilizing the cyber dimension, one can provide a response to any vital information, even complex information. However, it is possible to look at all the changes over the past few years as just "stretching logic," which means that the main mission and main concept have not changed. [84]

In Essence (General Perspective)

Intelligence in the era of artificial intelligence represents another leg in the journey of clarifying the concept and using intelligence and operational superiority (in context and for specific missions) in the Digital Era. The concept of intelligence in the DE can be summarized thus: to apply the potential of the Digital Era to the systemic challenges that intelligence now faces. Alternatively, a different concept of intelligence-operational superiority, based on the understanding that the information explosion and the ability to strive to know "everything about everyone" makes an updated and different intelligence and operational response both possible and required. [85]

The intelligence endeavor in the DE can be described as a different approach to intelligence (and operational) superiority. For example, Google's approach to the information explosion is different from that of its predecessors. One day a friend showed me a joke that was circulating on the network:

Q: "Where is the best place to hide a corpse?"

A: "On page 2 of a Google search, where it will never be found."

This joke is kind of an "aha!" moment" and captures the truth of the matter quite simply. As intelligence personnel, over the years we grew accustomed to reading hundreds and thousands of items to find a piece of a puzzle in one of these items, and then we tried to connect it to another puzzle piece in another item. Finally, we would try to construct the full picture. In actuality, most of the items do not necessarily contribute in any particular way to understanding the whole. Hence, the task of the research officer is to "separate the wheat from the chaff" and find the relevant data from within the mountains of items.

Google has a different approach. When I ask Google a specific question (and have not just woken up in the morning and begun reading through the myriad news items that arrived during the night), I am not prepared to

go to page 2 of a Google search and read the title of one of the answers that appears there. I expect Google to provide me with the answer on the first page and in one of the first titles. I don't look at the second page. If I don't get an answer, I don't despair, and certainly don't say to myself, "Okay, Google doesn't know." Instead, I say to myself, "Google knows everything, but I didn't ask Google the right question." Moreover, Google has never asked me to prioritize one population group over another. Google presumes, under the aegis of the Information Age, to know everything about everyone, even if that means knowing everything about billions of people. [86]

In a nutshell, this needs to represent the novel approach of intelligence in the DE. Superiority does not stem from one or another piece of information, but rather from the information explosion itself and the ability to ask about whatever interests me. When the information is truly infinite, then clearly one cannot expect to read all the items, and there is no need to reset the columns. The approach is different. One can and must wander among the bits of information. According to this approach, the answers can already be found in the existing information. One just has to know how to optimally navigate through it and ask the questions that interest the intelligence officer. [87]

Keeping in mind the limitations of the metaphor, we can liken the situation to the global breakthrough that occurred around the cracking of the Enigma Code. Even before then, there were geniuses who deciphered codes, but the British and the Americans knew that cracking the Enigma Code would require 20,000 people who would have to work for 20,000,000 years. Therefore, they built a machine to help them crack it. This machine was the first step in the invention of the supercomputer, which changed the course of human history. This is similar to what is happening in our era when it comes to information, its use, and its significance. [88]

Hence, the intelligence analyst continues to be relevant (the relevance and importance have actually increased), but the conversation between human and machine is changing. Due to the fact that AI is accelerating the DE Revolution, it is also accelerating the revolution of the intelligence organizations as we know them. In other words, we can frame it with the understanding about traditional learning and synergetic learning. Intelligence is a process of learning about your rivals and enemies. The Human-Machine Team, which creates synergetic learning, is a new process of learning as well as a new way to shape and to influence. [89]

The Importance of the Question

Throughout the years, Jewish tradition has encouraged its people to know that asking questions is their right, their responsibility, and even their duty. This encouragement to ask questions is exemplified by the Four Questions that are asked at the beginning of the Passover Seder meal and are the basis for the retelling of the entire Exodus story. Intelligence, too, focuses on the responsibility to ask the right questions, thereby making it possible to pinpoint precise, vital bits of information and clarify a complex reality. These questions provide a fundamental compass for intelligence activity.

According to the traditional approach, any successful question can lead to relevant accessibility, thereby exposing the secrets of the other side. If it is a question to which there is no answer in the available information, deep insights can still enable us to identify the adversary's logic, thoughts, and so on. In the era of information explosion, however, one can assume that for (almost) every question, a possible answer can be found in the data. One needs to know how to probe the data for the right items, construct questions that can contend with the information load, and understand that when an answer is not obtained, we must assume that we have not asked the right question. [90]

If the foundation of the information has been properly organized, the main thing we have to do is improve our ability to ask relevant questions. In addition, one can relate to a question that was asked by someone else as a potential feature for The Human-Machine Team. If an analyst searched the information about a certain matter and the information was understood in a specific way, this can reveal something new about the information. For example, if an analyst checked who was usually asleep at 11 p.m. and in the last month was awake between 1:00 and 4:00 a.m., both the question and the answer can be new features to identify indicative signs. Another example is if an analyst checked all the new greenery planted in a specific area in which it seemed that there was no reason , this knowledge can also be an indicative sign for this location. Each month, intelligence organizations ask hundreds of thousands of questions that produce hundreds of thousands of answers. Combined, these questions and answers create potentially relevant features that we can use to upgrade the power of The Human-Machine Team to achieve impressive capabilities of machine-learning. The new knowledge can also be created from combining a few questions. For example, an analyst could decide to check all the suspects who did not sleep in their homes during the last two nights in a specific area, and who also discussed weapons purchases during the past week. This question, plus the names of the suspects produced by this question, can now be a combination of "relevant features" for machine-learning. As discussed in the section about machine-learning, the more features that can be provided to the machine for the process of learning, the better the results. [91]

Intelligence in the Era of Artificial intelligence Automation

The first new opportunity is to automate intelligence processes in a way that can create new abilities that were not been possible before. Under this

umbrella, there are new opportunities to do the same things, only faster and on a larger scale. For example, Speech-to-Text (STT) can replace audio-lingual analysts. Today, intelligence organizations have thousands of audio- lingual analysts. They are required to listen to enemy discussions or read enemies' internal data and translate the original language back to their countries' native languages. The idea behind STT appeared decades ago and has not been replaced. Today, we have the conditions and the abilities to fulfill this concept. In five years, we will still need audio-lingual analysts, but more than 80% of their tasks can be replaced by machines. Another example is machine-learning to replace image and video analysts. Similar to audio-lingual analysts, every intelligence establishment has thousands of image and video analysts. Recently, AI machines have been learning how to replace some of these analysts' functions. Furthermore, in this area, we also have the conditions and abilities to fulfill this idea and carry out tasks using AI machines.

Completion of Puzzles That Were Previously Unsolved

A "havruta" [92] of The Human-Machine Team creates new ways to solve puzzles that were previously unsolved. One of the new abilities to enable this new potential to use AI to solve puzzles is based on "the power of the internet." Intelligence organizations previously used unique capabilities to acquire classified data. Over the years, we got used to the fact that the big secrets were found in isolated offices. Similarly, in the cyber era, the prevailing notion is that the major secrets are harbored in classified "internal networks." Accordingly, in many cases, the more intimate and internal the information, the more difficult it is to obtain this information, the higher its classification – and usually its relevance as well. For us, in the Information Age, the greatest challenge is not necessarily the ability to create intimate accessibility of one kind or another, but the ability to

exhaust the relevant information within the infinite amount of information in general, and on the internet in particular. [93]

It appears that intelligence organizations have not yet achieved this revolution and certainly have not internalized it. Great efforts are still being invested in creating additional accessibility. However, we assert that whoever wins the competition to leverage the existing information on the internet on behalf of their own organization's intelligence challenges will be a step and a half ahead of other organizations. [94] One of the secrets of success in the coming years will be precisely the ability to use the power of the internet to the benefit of the security intelligence entities. [95]

Influencing and Shaping Reality

In the DE and in the Information Age, data is part of the reality. In other words, when we influence the data, we alter reality. This is a novel, basic situation for the intelligence establishments. Intelligence organizations have been using data, for the most part, to make recommendations. Today, due to their responsibility over data and expertise with data, intelligence organizations have the opportunity and responsibility to shape and transform reality. "Influence or shaping effort" in the period of The Human-Machine Team is a new opportunity for intelligence organizations. This mission includes intelligence for shaping reality, and not only for describing it.

The Digital Era, and specifically social media, have established a new reality in which facts and fake realities are blurred. Thomas Friedman described it thus: "I fear we are seeing the end of 'truth,' that we simply cannot agree any more on basic facts…what we are experiencing is an assault on the very foundations of our society and democracy, the twin pillars of truth and trust." [96] From time immemorial, people have attempted to shape reality. Beginning in the Garden of Eden, Adam tried to

"influence" God's thinking about what exactly happened. The development of media, and especially social media, dramatically augments the potential to shape reality. [97]

Today, anyone can be a sort of media station with his or her own smartphone. The ease of tweeting, posting, and texting made the "influence effort" a relevant part of the "act of war" as well. The influence or shaping effort also has the potential to be a decisive factor in victory or loss. The shaping effort in the period of AI can be much more relevant. For example, machine-learning can help create "influence in context," which means that different audiences and different individuals will receive the relevant data from the relevant media that has the greatest chance to influence them. This new concept also requires different people and cultures. Russia is an example of a country that is becoming more and more active in using data to influence reality. An extreme example is the accusation that the Russians influenced the 2016 U.S. presidential election with a data campaign that possibly included AI capabilities.

New Potentials and New Opportunities for Our Enemies and Rivals

The first risk is that our enemies and rivals will be a few steps ahead of us and will take the lead in this competition of artificial intelligence. The free world that led the Industrial Revolution has also succeeded in leading in cyberspace. The U.S. and U.K., as well as Israel, have achieved cyber advantage. Currently, Russia and China have marked AI as a field in which they plan to lead on a global scale, and have invested resources to accomplish this goal. "AI is the future not only for Russia but for all humankind…whoever becomes the leader of this sphere becomes the ruler of the world." These resounding words, spoken by President Vladimir Putin in September 2017 to students on their first day of school, show why we need to keep at least a few steps ahead of our enemies and rivals in this

field.

When we speak about cyber, the strongest capabilities are still "government capabilities." When we speak about AI, the greatest capabilities are in the private sector. Therefore, our enemies and rivals can be a few steps ahead by simply purchasing and utilizing the best systems from the private market. The key to addressing this risk is to create novel ways to collaborate between cyber capabilities and AI capabilities. [98]

We Don't Have 70 Years

As we discussed, the idea of artificial intelligence, which first appeared 70 years ago, has begun to change our lives only during the last few years. The development of the foundations (channels) for big data that enable us to use all of the data allows us to take the idea of machine-learning and create the conditions to fulfill the concept of AI. [99] Therefore, it is a risk for security establishments that it will take another 70 years to fulfill the concept of AI in their organizations. The factors that have changed, and now help us realize the concept of AI, have not yet been implemented in security establishments. The first difference is the need for "channels" for a great amount of classified data. The second difference is the process of machine-learning that requires thousands of experiences. However, each conflict or war is a singular event, so we don't necessarily have relevant experiences for any particular war. The third difference is enemies who try to confuse the conditions and prevent the ability of the machine to learn from the past to make predictions. The risk here is that security establishments will become confused by the differences, and this confusion will prevent them from embracing the potential for the future. [100]

The challenge and the risk stem from trying to develop just "one floor" of the required changes without building all of the floors simultaneously. If someone tries to build AI machines without a systematic effort to first

organize the data, it will fail. On the other hand, the data to be organized is infinite and the task of organizing the ground floor will never be complete. Therefore, the risk is that we will spend decade after decade organizing the data without taking our organizations to the future of artificial intelligence. In addition, each war or conflict is a singular event, but the data is not singular; therefore, we need to use the data to address the singular event and build models based on the data for the conflict/war, and not based on the characteristics of the event. [101]

From the Data Perspective: Unmonopolize on the Data

Traditionally, intelligence organizations have had a "monopoly on the data." Most of the relevant information is classified. The unclassified information is not useful without the classified, resulting in the intelligence organizations' monopoly on the data. For years, intelligence bodies avoided transferring information to operational entities out of concern that they would make improper or irresponsible use of it. Similarly, even within the intelligence community itself, the collection units did not transfer most of the raw information to the research units. This was supposedly done for reasons of compartmentalization, but also for practical and doctrinal reasons. According to the approach used in the past, if one provides access to raw visual information about complex decoding to everyone, they may make improper use of it and jeopardize sources. Making SIGINT (signals intelligence) information available to analysts was viewed the same way. In the Information Age, however, there is no ownership of information; it should belong to everyone. For comparison's sake, no one avoids making medical information available on the internet out of fear that, God forbid, I may make improper use of it if I need the information to treat one of my children. Basically, the information belongs to everyone, and anyone can ask whatever they want and decide whether and when to turn to an expert

or make decisions by themselves. [102]

The monopoly of data creates difficulties during routine times of operation, but the difficulties intensify in times of major crisis and war, which are based on the independence of the various forces. The ability to use data in war is based on having the independence to access it. The reality in which intelligence organizations have a monopoly on their data (and other military organizations do not have the data in their information systems) does not enable the effective leveraging of the data. It is an illusion to think that intelligence organizations know how to use the data for the other military organizations. As intelligence organizations, we have to say good-bye to the ownership and monopoly on data without diminishing the responsibility to keep the classified data as confidential information.

Continuity of the Data

In the DE, the capabilities to create the necessary manipulations and the intelligence investigations are based on continuity – that is, the continuum between the kinds of material, various kinds of information, and various intelligence entities. Traditionally, different kinds or types of information could be analyzed separately, and then a human analyst could try to connect them into one picture. This is also the idea of intelligence as a process of putting together a puzzle. Data science is neither a branch of SIGINT (signal intelligence) nor an extension of VISINT (visual intelligence); neither is it an updated way to do research. Data science requires, and is conditional on, continuity and the ability connect the dots of different kinds of data in one processing of the data. Furthermore, according to this approach, even when there is 80% continuity in the data, there is a possibility that without continuity of the other 20%, all of the information will be worthless. This is because the real power lies in the ability to ask, and to clarify, the continuum as a whole. For example, we

have to structure intelligence so that we can ask machine-learning questions according to the following formula: who a person is (1) who spoke to someone in Iran (2) and lives 100 meters from a suspicious place (3) and was observed during the past hour (4) driving north (5) and did not sleep at home last night. This query pertains to various kinds of sources. What is needed is the ability to manage and clarify investigations of this kind. [103]

"Targets Machine" – A Game Changer to Achieve Victory in War – Case Study (1)

From Data to Prediction

Machine-learning is a technology to learn through the big data that you have to generate the information you don't have. Machine-learning for manufacturing targets means discovering unknown places and figuring out thousands of new targets. A "targets machine" uses data to answer questions about your enemy's hiding places and to draw conclusions from data to make predictions. This machine has new potential to deal with big data that a human brain cannot do alone. [104] The process is built upon several steps, each one occurring after the other. The main steps are gathering data, preparing it, choosing a model, training, evaluation, hyperparameter tuning, and prediction. [105]

It's All About the Data

Nowadays, almost everyone is personally targeted by machine-learning – not to discover the location of your missiles, but when Facebook uses machine-learning to suggest possible friends. Basically, it is similar when we discuss the targets machine. *The first step* is the data. The machine needs enough data regarding the battlefield, the population, visual information,

cellular data, social media connections, pictures, cellphone contacts, etc. The more data and the more it is varied, the better. Then, in *the second step* , the data needs to be organized in a way that a machine can access and process it. This includes the servers, the way in which the information is stored, and the ability to link between various elements of the information. The basis for everything is data. Without enough relevant data, without varied data, without preparing the data in a way that the machine can process it, nothing will be achieved. Many failures to build machine-learning have occurred because of problems with data. Data is the key to success. We can say that when we talk about the idea of "data science," the "data" are more difficult and more critical than the "science." [106]

Model

The next step is to choose and create a model. For example, the Facebook model shows how a machine can take the data and learn about potential friends. A targets machine needs to build a model to create new targets and figure out whether or not they are manned. It can be a model that includes a few strong features based on classified data that enables the connections of specific pieces of information to specific places on the map. In addition, it can be a model that builds on a lot of small, diverse features – hundreds or even thousands of them. For example, people who are with a Hezbollah member in a WhatsApp group, people who get new cellphones every few months, those who change their addresses frequently, etc. In this example, the power will be from the quantity and variety of different features. The model can be built by analysts, and at least part of it can also be built by a machine.

The model will be more complicated. The best option is to build the model with a few strong features and with a large quantity of varied features. A strong model will then be created through a control group of

targets that we know for certain already exist. Finally, after gathering the data, preparing and organizing it, and choosing and building a model, the first floor of the target machine is ready.

Training and Tuning

After we have a model, we can go to the *next level* of training and tuning. Training the machine involves checking the model and improving the machine. You can think of it like a runner who wants to improve his or her speed by studying running styles. After choosing a model to improve the style, he/she needs to train, using the model again and again. The importance of training is to check the model, improve it, and be more precise. When building the targets machine, after we have the model of new targets, we can begin the training. We can take the model and start to check it again with the data. The training will help improve the machine, check if the features work, and find the relevant targets. During the training, we can improve the model's accuracy.

For example, this process can help understand whether the model gives more priority to picture patterns than to other features, and because of this focus, if there are mistakes. As a result of training, we can make small changes to a few parts of the focus or to the priorities of the model. When we finish the training, we have an improved model.

Evaluation

The next step is evaluation – which means jumping into the real world. Evaluation is testing our model with data that has never been used for training. The results never have 100% compatibility with the model. This step is first to determine if we have a good model for a targets machine – or not. Usually a 70% or 80% match is good enough. This step also helps

improve the model, which is why the step after training and evaluation is tuning, specifically "hyperparameter" tuning. The testing in the real world helps to choose the hyperparameters and give them more weight in the model.

A targets machine can use the model with data that has never been used to check places and find new targets. The end of this step is the option for hyperparameter tuning. For example, if we see during the evaluation that one feature is stronger than the others, we can decide to give this feature more priority. This is the second floor of machine-learning: training, evaluating, and tuning. Now, when we have data and the improved model, we can go to the final step of prediction. [107]

Prediction for a "Targets Machine"

Prediction is the step when the machine can begin to answer questions. For our example, we can put classified and unclassified data in the model, and the machine can start to think and suggest new targets. Prediction is when the value of a targets machine is realized. Agrawal, Gans, and Goldfarb in their book, *Prediction Machines,* give an amazing definition of prediction:

> "PREDICTION is the process of filling in missing information. Prediction takes information you have, often called 'data' and uses it to generate information you don't have." [108]

From their perspective, prediction is a fundamental ability of human intelligence, and prediction can generate information about the present and the past. [109] Usually, we think that prediction is for the future. For me, understanding that prediction is first of all about the past, and the present was a real "aha!" moment.

Usually, machine-learning takes place when there is data that we have that provides data or information that we don't have. Only the activities will

be in the future, but the conclusions are from the past or the present. A targets machine can learn from the data and the information it has about Lebanon and Hezbollah, and suggest new places where rocket launchers may be hidden.

The Human- Machine Team to Address Lone-Wolf Terror Attacks – Case Study (2)

Artificial intelligence also has the potential to influence the continuous campaign (sometimes called the campaign between wars). The Human-Machine Team can also influence the ability to find terrorists before they commit a terror attack. One major example of a type of crisis that intelligence organizations in Israel face is the phenomenon of "terror by inspiration," which takes the form of lone-wolf terror attacks. A potential terrorist wakes up one morning and decides to perpetrate an attack using a kitchen knife to stab a victim, or the family vehicle to run people over. Sometimes the person doesn't even know a day before that he or she is going to commit such an attack. In these cases, traditional intelligence agencies are helpless. How can such an attack be predicted or prevented? What can be prioritized as an essential piece of information to be monitored in lieu of something else?

Indeed, time after time we have found ourselves without a relevant, adequate response to lone-wolf terror attacks. The crisis was so severe in Israel that in October 2015 we found ourselves going from terror attack to terror attack and from funeral to funeral. Each time we said to ourselves in retrospect, "Wait a minute! There must have been some sort of indication here that, if we'd paid attention to it, maybe the attack could have been prevented." As time went on and the intelligence units continued to be irrelevant, the sense of crisis intensified. We realized that the superiority [110] of the intelligence agencies to address terror attacks in advance was indeed

being challenged. We understood that when it came to terror by inspiration perpetrated by lone wolves, the way we had done our intelligence work over the last decades was insufficient.

Since everyone has the potential to be a lone-wolf terrorist, it is impossible to check all of the people all of the time. A mission like this, similar to solving the Enigma Code, requires more than 20,000 analysts and more than 20,000,000 years. The way to tackle this complicated challenge is with a team consisting of humans and machines, and through the "bounces" and "passes" between this human-machine team. The first step is human. Humans must identify the limits and give examples of characteristics from past lone-wolf terrorists. Then humans and machines together need to formulate the characteristics of potential terrorists, using experience from the past to make predictions for the future. The next step is the prediction that a machine creates through the big data about specific suspects. Finally, humans check these suspects and decide how to act. This concept and process has helped us address these challenges and to prevent tens of lone-wolf terror attacks every month.

The Human- Machine Team for a "Smart Border" – Case Study (3)

A "smart home" is an everyday example of the new capabilities based on AI that are accessible to homeowners. A smart home uses various types of data in one specific place to improve the quality of our lives by using bits. Digitization creates the ability to represent, arrange, and process the real world through bits. The great jolt that changes our lives is the ability to take different kinds of data and transform them into binary digits. AI has the ability to take all these bits and use them within the context of a specific place, thus transforming a "normal" house into a "smart" house. The idea of a smart area is to use The Human-Machine Team to protect places such as our borders. The ability to connect the bits around the border through

machine-learning can help control and protect them. (Another example is a "smart movable protected area" that friendly forces operating in enemy territory can utilize to better protect themselves from multiple threats.)

The basis for a smart border is the connection between the place and the person who does something in it (intentionally in that order, i.e., starting with the place). In the DE, one can fuse visual information and networked information in a given spatial cell. This fusion can deal with a warning, and in general help provide a different response to operational needs in a geographic context. The smart border begins with defining the space. Its starting point is the choice of the spatial cell we optimally want to reach (it could be across the border, or where there is suspicious activity, etc.). Within the specific spatial cell, one must create the ability to fuse the various sensors within the context of the operational problem that has been defined. For this spatial cell, it is also necessary to organize all the data within the context of that same location. In addition, we must organize task-specific sensors, and attune an intelligence and operational entity to utilize the information of the smart space. All of these factors together can achieve an improved operational response.

We can begin to build a smart border by choosing a section of the border and building a proof of concept. The first step will be to organize all the data on this area: history, familiar faces in this area, geographic layers, etc. Second will be to organize various kinds of sensors to "control the area" – e.g., cameras, registering cellular identities, drones, etc. The third will be to build a system to connect the different types of data to each other; the fourth to design machine- learning to identify unusual phenomena and, lastly, to build an analyst group to deal with this machine and improve the smart border every day based on every experience.

---

73 Keens Van der Heijden, *Scenarios : The Art of Strategic Conversation* (West Sussex: 2010 publisher?) xv, xvi.

74 A few references will be from the Israeli perspective in a war against Hezbollah and its supporters (the largest national security threat to Israel). However, it can be relevant with updates for other rivals and enemies.
75 Yuval Noah Harari. op. cit., 179-181.
76 The Sinai Campaign (also known as the Suez Crisis, or Sinai War) was Israel's invasion of Egypt in late 1956, with later involvement of the U.K. and France . The aims were to regain Western control of the Suez Canal and to remove Egyptian President Gamal Abdel Nasser , who had just nationalized the canal.
77 Yuval Noah Harari. op. cit., 166-169.
78 Yuval Noah Harari. op. cit., 16-18, 172; Ray Kurzweil, op. cit., 382-390.
79 "Intelligence factory" is the ability to use data and information to manufacture more and more targets. "Fire factory" is the ability to attack the targets at the right time and with the right kind of weapon.
80 On the potential to make decisions, see Ajay Agrawal, Joshua Gans and Avi Goldfarb, "*Prediction Machines : The Simple Economics of Artificial Intelligence*" (city? Harvard Business Press, 2018), 73-82. On the question "Can autonomous weapons be used safely?" see Paul Scharre, *Army of None* (New York: W.W. Norton & Company, 2018), 161-168.
81 Paul R. Daugherty, James H. Wilson. op. cit., 138-140.
82 Kuperwasser, Yossi and Siman-Tov, David. "Intelligence in Theory and in Practice," *Big Data and Intelligence* (a Journal on Intelligence Methodology, October 2018), 4-9.
83 There are, of course, other ways in which proper intelligence activity has been described over the years. Here, though, we have sufficed with a relatively well-accepted description. In any case, the change that we will describe below, in the context of the new approach of the Information Age, is different from every other way in which intelligence has been described over the years. The issue of pointing to vital information appears in all of the different approaches.
84 Col. Y. "Intelligence in Theory and in Practice." *Big Data and Intelligence* (a Journal on Intelligence Methodology, October 2018), 10-12.
85 Superiority is always in context and specific for each mission, and not a general perspective.
86 Ajay Agrawal, Joshua Gans and Avi Goldfarb. op. cit., 10.
87 Thomas W. Malone. op. cit., 189-191.
88 Col. Y. op. cit., 10-12, 22-23.
89 Thomas W. Malone. op. cit., 231-241.
90 Ajay Agrawal, Joshua Gans and Avi Goldfarb. op. cit.,191-194.
91 M. "Angels in the Skies of Berlin: New Intelligence Questions in a World Steeped in Data, Intelligence in Theory and in Practice. *Big Data and Intelligence* (a journal on Intelligence Methodology, October 2018), 62-68.
92 "Havruta" is an Aramaic word meaning "friendship" or "companionship." It is a process of synergetic learning between humans who study and learn together as a team.
93 Thomas W. Malone. op. cit., 175-184.
94 Intimate and classified networks are not yet available on the internet. However, the ability to use all the power that is on the internet will be a unique advantage in the coming years. (Intelligence organizations used to act to achieve classified data and don't didn't? put effort into using the internet's inherent power/)
95 Col. Y. op. cit., 17-18.
96 Thomas Friedman, "*Where Did 'We the People' Go?*" New York Times, June 21, 2017,

https://www.nytimes.com/2017/06/21/opinion/where -did-we-the-people-go.html
97 Yuval Noah Harari. op. cit., 236-241.
98 Yuval Noah Harari. op. cit., 74-77.
99 Chapter 1 and specific FN 44 (brief history of AI).
100 Paul R. Daugherty, James H. Wilson. op. cit., 166-172, 180-181.
101 Ajay Agrawal, Joshua Gans and Avi Goldfarb. op. cit., 202-205.
102 Different kinds of information are protected, and there are secrets that people and companies don't want to put on the internet. However, this information is kept off the internet due to issues related to privacy and policy, and usually not for ideological reasons.
103 Haim Assa. "Advanced Data Retrieval in the Big-Data Era, Intelligence in Theory and in Practice." *Big Data and Intelligence*" (a Journal on Intelligence Methodology, October 2018), 40-47.
104 Executive Office of the President National Science and Technology Council Committee on Technology. op. cit., , 8-9.
105 Stuart J. Russell, Peter Norving. op. cit., 244-247.
106 Ajay Agrawal, Joshua Gans and Avi Goldfarb. op. cit., 40.
107 Ajay Agrawal, Joshua Gans and Avi Goldfarb. op. cit., 38-40, 45-47.
108 Ajay Agrawal, Joshua Gans and Avi Goldfarb. op. cit., 24.
109 Ibid p. 30.
110 Superiority means being a few steps ahead of your enemies. "Intelligence superiority" means having much more knowledge about your enemy than your enemy has about you (its plans, forces, systems control, etc.). This means superiority within the context of a specific issue or mission, and not general superiority.

PART 2

FAST

FOUNDATION,
ACCELERATION ,
AND SINGULARITY TIME

CH APTER 4

Challenges and Difficulties

Today's nations and organizations were developed with characteristics and culture that matched the Industrial Revolution. However, the DE is a novel, high-level paradigm, and because of AI, we are on the threshold of the acceleration of the DE Revolution. As a result, nations and organizations need to adopt a digital transformation strategy for this era. [111] This transformation is a huge challenge. The future belongs to nations and organizations that will succeed in dealing with the new challenges and difficulties that arise due to the era of AI.

In this book, we focus on the structural and cultural challenges for digital transformation in the security establishments. The first step is to address the challenges for digital transformation that organizations in various fields of interest are facing today. [112] Furthermore, there are additional, unique challenges for security establishments, for which there are at least three reasons: 1) the culture of the security establishments; 2) the characteristics of the security mission; and 3) the necessity to use infinite amounts of classified and unclassified data at the same time.

Intelligence organizations have unique challenges because they have a responsibility to deal with both "the secrets" and "the unknown." Information and knowledge are at the core of intelligence organizations. In addition to their internal work, these organizations also need to communicate with all branches of the military and with other intelligence organizations. To complicate matters, all this communication goes on at the same time on the same network. As a result, intelligence organizations have built-in challenges to achieve digital transformation. It is challenging to be part of the military network, guard the secrets, and deal with the unknown

all at the same time. Despite the challenges, intelligence organizations must pursue and succeed in their digital transformation programs. Those that do not succeed at this will also fail to accomplish their goals. [113]

Six Unique Challenges

The first and most complex challenge is to build a "closed-open-closed" network. Is it possible to develop a closed network that is actually an open network at the same time and on the same network? Such a network is, on the one hand, a closed network that nobody outside the system can access, and on other hand it behaves like an open network to access the entire internet. In other words, closed to the outside world for classified data, open for the security organization to connect the internal classified data and the external unclassified data, and closed after the classified and unclassified data are merged. A further advantage of this system is that every member of the organization can also use his or her private smartphone to access the internet. For a day-to-day example, we can ask how it is possible to build a network in which someone who works for a security organization can take a picture with his private smartphone, send the information to the classified network, and merge it with the classified data. (In this example, the network must be open to send the picture and then closed due to the classified data.)

A closed-open-closed network means to enable infrastructure to build machine-learning in such a way that part of the data will be public from the internet, and part of it will be classified information that is not on the internet. The machine can then use the different types of data at the same time. Such a network means that the private classified cloud and the public cloud can communicate with each other all the time without the user experience being compromised. A closed-open-closed network means that security organizations can operate from public places such as WeWork, [114]

and at the same time use an internal security network.

It is necessary to build a closed-open-closed network so that security organizations can continuously and simultaneously deal with classified and unclassified data as part of their daily routines. Today, most of the information and knowledge that security establishments need to operate on a daily basis is unclassified. However, the classified data is critical. More often than not, the infinite amount of unclassified data is irrelevant without the classified data. At the same time, the classified data may have substantial gaps without the unclassified. Some security organizations simply copy information from the internet to the internal network, but this provides only a partial solution that leaves large gaps. Today, the ability and the potential for people and machines to reorganize the different types of data is a required condition to successfully address security challenges. [115]

The second challenge is the requirement to build a cloud for a large amount of classified data. In the past, we did not have enough data. In the current reality, due to the Information Revolution, security establishments also have big data. Since a lot of this is secret, security organizations use private servers. However, to deal with all the data, we must migrate to the cloud. Today there are clouds for a great amount of data only in companies such as Amazon, Google, or Microsoft. [116] How can the security establishments use the "Amazon cloud" and feel secure? How can this public cloud communicate regularly and securely with a private cloud? The foundations of the information infrastructure are the unseen, yet indispensable sewer pipes (the channels for data) that – if compromised – make the neighborhood unlivable. Clouds are an important component of this information infrastructure. Without a good solution for clouds, and without a systematic and thorough treatment of the "channels," digital transformation in security will fail. In other words, without the ability to store the data (including classified data), and without the ability to use this

data easily for various missions, nations and organizations will not successfully make the AI Revolution real. The decision of the CIA to work with the Amazon cloud is just the first step. [117]

The third challenge is the fact that in the security establishments, different organizations use different networks. From time to time, different departments in the same organization even use different networks. For example, the Air Force uses a different network than the intelligence agencies, the Army uses a different network than the Navy, and so on. It is difficult for organizations to give up using their own private networks, since a network is the basis for an organization's independence. Today, a good network is a condition for success. Usually, organizations feel that they cannot trust anyone from outside their organization to build and operate their network. Consequently, how can different organizations with different networks feel and act like they have the same network? How does the concept of the "flat world" manifest in security organizations that have different networks, and where every organization has its own secrets? [118]

The fourth challenge is due to the mission. How can security establishments achieve this complicated, challenging transformation and at the same time be prepared for war? How can security establishments reach the next high-level paradigm and at the same time be prepared to achieve victory in a war that is based on the existing paradigm? One of the main characteristics of a military organization is the responsibility to be prepared for war at all times, 24/7. The possibility that a war may erupt at any given moment makes preparedness the top priority.

For example, the Second Lebanon War that Israel fought against Hezbollah in 2006 broke out when the IDF was in the middle of transformation. Therefore, along with many achievements, difficulties broke out during the war, owing to the fact that it broke out in the middle of this transformation process. The IDF had one foot in the past and one

foot in the future, and thus there were challenges. In the public market, when you build the next generation, the previous generation continues to behave as it behaved before, and you just stop training to improve the old model. For example, when Apple works on the next generation of the iPhone, the previous iPhone continues the way it worked before. However, in the military, we need to build the next generation and invest time and money for this purpose, but at the same time we must be prepared for the supreme test of war. It is a huge challenge to take your organization to the future, while simultaneously improving your preparedness to win a war that can erupt at any minute. Part of this challenge is that you need to keep and utilize your previous abilities while transforming the organization for the use of next-generation abilities. Finally, it is very difficult to dream up the innovation, do the transformation, and improve your preparedness in the same organization with the same resources.

The fifth challenge is due to the organizational DNA of the learning process in the security establishments. Digital transformation means taking your organization into the future. It also means taking advantage of new opportunities that the DE provides. Historically, national security establishments learn, first of all, from crises. An effective way to learn in military organizations is from a turning point. These organizations do not usually learn from potential opportunities to succeed, which is usually the normal process in the private sector. Security establishments are constantly in the process of addressing big challenges; in addition, they are usually hampered by a lack of resources, which is the reason that it is so difficult for them to invest money based on abstract issues for which they do not know exactly what the return will be. This is especially difficult when security establishments have concrete issues and emergencies to which they must allocate their precious resources.

This is but one of the reasons that most of the changes in security

establishments take place only after crises. In addition, it is difficult, if not impossible, to conclude that the crises arose as a result of data. Information is everything – and everything is information. Since information is everything, it is hard to identify the crises that occurred due to problems around data infrastructure. The bottom line is that security establishments are used to learning from crises, and it is challenging to understand that there was a crisis because of data.

Th e sixth challenge is the cultural challenge to use outsourcing capabilities before inside abilities. Over the last few centuries, security establishments used to be the "No. 1" source to develop weapons and invent military capabilities. For example, the U.S. Air Force is also the force behind the acceleration of airplanes for use in the private sector. The best airplanes are always in the Air Force (companies such as Lockheed Martin and Boeing are a kind of "inside ability," because even though they are considered industry, the company "in essence" is part of the U.S. security system). In the digital fee, it is just the opposite. The free market will always have much more money, data, experience, and manpower to enable it to be at the forefront of digital technology.

In digital transformation, outsourcing capabilities are crucial. For digital capabilities in the security establishments, the concept of outsourcing needs to be like the concept of "inside abilities." Typically, security establishments use outsourced capabilities for approximately 20% of their products and required capabilities; to succeed in the Digital Revolution, they need to use outsourcing capabilities for 80% of their products and outputs. The bottom line is that national security establishments traditionally use "inside units" before "outside companies." To deal with this challenge, we must change our culture. [119]

Three More Challenges from the Perspective of War

A war is a singular event. By contrast, machine-learning is a continuous process that is based on the ability to learn through big data from both the past to the future. [120] The process of machine-learning is built upon several steps, each one taking place after the other. [121] During war, however, everything changes. In addition, the desired outcome is not to lose the war and then to prepare for the next one by learning from the defeat. New data will be acquired during war, and obviously we cannot gather and prepare for data that we do not yet have. The ways the enemy will act during war will change, so it is also impossible to choose a model based on experience from previous wars and use it during a current war. Is there a way to use AI in a singular event?

The mode of operation in war reveals an additional challenge. How can we "run the war machine" when there is a "monopoly on data" and a "monopoly on firepower?" Intelligence organizations have a monopoly on the data; most of the relevant information is classified, and the unclassified information is not useful without the classified. The result is that this monopoly creates difficulties during routine times of operation, but the difficulties intensify during a crisis (or war). War is based on the various forces acting independently. The ability to use data in war is based on having the independence to access it. The reality that intelligence organizations have a monopoly on their data (and other military organizations do not have the data in their information systems) does not allow the option to leverage the data in these other organizations. It is a delusion to think that intelligence organizations know how to use the data for other organizations. The second part of the problem is the monopoly on the firepower capabilities effort. [122] For example, there are capabilities that only the Air Force has, and only those in the Air Force have the responsibility and the ability to use them. The reality that other organizations have a monopoly on the data, and a monopoly on the "fire,"

precludes the ability to use the data in all of its power and realize its full potential.

Finally, when we address life and death during war, we must take into consideration the legal aspects as well as the ethical perspectives. Are we going to take human lives based on AI? Are we going to attack a manned target (with people) just because machine-learning decided that this is the right time and place to attack?

---

111 Congressional Research Service on "Artificial Intelligence and National Security." (April 2018), 24.
112 On liability risks, quality risks, security risks, input data risks, training data risks, and feedback data risks see Ajay Agrawal, Joshua Gans and Avi Goldfarb, *Prediction Machines: The Simple Economics of Artificial Intelligence*" (Boston? Cambridge? Harvard Business Press, 2018), 195-204.
113 Baron, Eran. "Intelligence in Theory and in Practice." Big Data and Intelligence (a Journal on Intelligence Methodology, October 2018), 48-53.
114 WeWork is an American company that provides shared workspaces for technology startup subculture communities, and services for entrepreneurs, freelancers , startups, small businesses, and large enterprises.
115 Lt.-Col. T, "Intelligence in Theory and in Practice." *Big Data and Intelligence* (a journal on Intelligence Methodology, October 2018), 27-31.
116 Yoelle Maarek, "Intelligence in Theory and in Practice." *Big Data and Intelligence* (a journal on Intelligence Methodology, October 2018), 36-39.
117 Lt.-Col. T, "Intelligence in Theory and in Practice." *Big Data and Intelligence* (a journal on Intelligence Methodology, October 2018), 32.
118 Lt.-Col. T, "Intelligence in Theory and in Practice." *Big Data and Intelligence* (a journal on Intelligence Methodology, October 2018), 30-31.
119 Lt.-Col. T, "Intelligence in Theory and in Practice." *Big Data and Intelligence* (a journal on Intelligence Methodology, October 2018), 32.
120 Ajay Agrawal, Joshua Gans and Avi Goldfarb. op. cit., 23-28.
121 The main steps are gathering data, preparing the data, choosing a model, training, evaluation, hyperparameter tuning, and prediction. For more details, see Chapter 3: National Security in Between Paradigms, an example of "Targets Machine."
122 "Fire effort" includes the various capabilities to attack from afar, e.g., airplanes, missiles, artillery, etc.

CH APTER 5

FAST – A New Concept

This purpose of this entire book has been to reach this moment. In this section, our purpose is to guide the first steps toward realization of the dream of AI. What should we do to fulfill the potential of The Human-Machine Team, and what are the requirements to lead our nations and organizations to the era in which human intelligence and artificial intelligence merge? Our plan is called "FAST": Foundations, Acceleration, and Singularity Time.

The future belongs to the nations and organizations that will build the relevant foundations that enable the AI revolution. [123] These *Foundations* are (1) a campaign to acquire more and more data, both classified and unclassified, as much and as varied as possible; (2) the ability to store and tag all the data based on cloud technology; (3) a closed-open-closed network that deals with the classified data and unclassified data in the same system and on the same network; and (4) to build strong, broad computer power (specifically, to build the foundations with enough GPU servers to deal with a great amount of data). [124]

The idea of *Acceleration* means that no matter what happens, in 20 years our nations and organizations will possess substantial AI capabilities. Our responsibility is to accelerate the process and to bring (part of) the future into the present. Aggressive acceleration includes (1) empowering regional (edge) capabilities, which means choosing strong concepts and capabilities and empowering them by using AI; (2) automation of analysts' functions, e.g., automation to carry out tasks of image and linguist analysts; (3) automation of military hardware, including weapons, vehicles, and drones; and finally (4) collaboration between human combatants and robotics.

Initially, these collaborations should be formulated in small units. T he concept of *singularity time* means creating and establishing places (departments, units, organizations, and companies) that will focus on the distant future and on ideas that today seem totally unrealistic. [125] The purpose of this idea is to prepare ourselves for the future and help discover ideas from the future that will also enable the current acceleration of AI.

"Who Are We in the Era of AI ?" ("New Glasses")

We are the same people, but now we have "super-cognition." This means that challenges that were unsolvable in the past can now be addressed in ways that we could not have imagined before AI. The limits of cognition are changing, as are the rules. [126] We can and must check every issue also from the perspective of The Human-Machine Team. Cognition is one of the most important abilities to have created history. Therefore, when a machine can perform human cognition, it changes the potential for humans and machines to "think" together, thereby creating a kind of super-cognition. This revolution gives humans new glasses with which to look at every challenge, every concept, and every mission. [127]

Key Questions

To discover how countries and superpowers are reacting to the AI era, we should ask ourselves a few key questions. The general, and most important ones are what we need to do tomorrow to fulfill the potential of The Human-Machine Team; what is our vision for AI; and how should we achieve this vision? In addition, we need to ask key questions to understand the potential between AI and other fields, such as: AI and cyber; AI and the electromagnetic spectrum; AI and the intelligence organizations; and AI and the relationship between national security

establishments and the free market.

F oundations

- Fulfill the requirements necessary to enable the AI Revolution
- Ca mpaign to acquire more and more data
- Keep and tag all the data (cloud technology)
- A closed-open-closed network
- High-performance computing

Before we begin our journey to the future, we must understand that one cannot build a second and third floor without the first. A building without a foundation and without sufficient "sewer pipes" will be unlivable and can collapse. The first step to lead AI transformation (and the most complicated and important step) is to build a strong, stable, structural foundation for data. Until this system is built, we cannot begin the task of building the rest. This system needs to order the data and organize the relevant information. The data must be stored in the right places, but the aim is not to just appoint people to manage the information and be responsible for preserving it; the various databases must be connected and fused. In addition, we must decide which type of material will be preserved where, and so on. This begins by mapping what exists in the world, and what the data is in similar organizations and among us in our own organization. The process continues with organizing the relevant servers for this kind of data and crafting the organization's information strategy (which type of information is stored where, in what configuration, etc.). As noted, the importance of this step cannot be overemphasized. If one can invest in only one issue in the Information Age, it should be in the structure of the foundations of the information. Another way to convey the message is to note that in the data-science era, the data is even more important, complex,

and challenging than the science. [128]

Data is the first condition (prerequisite) for building an AI machine. The more data you have, and the more variety you acquire, the better. National security organizations have access to the data in the public domain, as well as classified data that only they possess. Therefore, national security establishments fulfill the condition of big data. In addition, the classified data itself is a great amount of classified and varied data; as a result, national security establishments have both the quality and quantity of data required to build AI machines. Data is the first foundation to lead this revolution, so our goal is more and varied data.

The second foundation is the *ability to store , label, and organize the data.* These abilities became a kind of non-issue in the free market, but they represent significant problems for national security organizations. These organizations deal with classified data, and therefore they don't want to expose their data in public clouds. Moreover, classified data is less relevant without the ability to merge it with unclassified data. The reality today is that national security organizations used to keep their classified data on private servers or private clouds, which means that they cannot take advantage of the capabilities of the public clouds that every individual and every company can enjoy. Furthermore, national security establishments have a considerable challenge to store, organize, and clean their data. In addition, it is a challenge to merge the classified and unclassified data as part of the same network. [129]

The third foundation is *high-performance computing.* During the last few years, high- performance computing has improved the ability to address large amounts of data, and therefore improves many organizations in the free market. High-performance computing is a resource lacking in national security organizations.

In addition, we must have *data analysts* to address the data. A data

analyst who focuses on the data (which kind we need, how to use it, on which servers, etc.) is a new position both in private companies and in national security organizations.

The bottom line is that the first step is to *fulfill the foundations that will enable the AI Revolution*. This step includes (1) a solution for storing and organizing all the data; (2) a continuous campaign to acquire more and varied data; (3) the ability to enable merging classified and infinite unclassified data. For this merger, we must build the national network as a closed-open-closed network. As discussed earlier, closed for classified data, open to connect the classified and unclassified, and closed after the classified and unclassified data is merged; and (4) to invest enough resources to ensure that high-performance computing is a non-issue. The first step towards achieving high-performance computing is building the capacity of GPU servers in the security establishments. [130]

For comparison, we can look at the following table; it compares the current preparedness of national security establishments to fulfill the AI Revolution and the ability of the free market to implement it.

	Industry + Free Market	National Security Establishments
Data	✓	✓+
Ability to Store and Organize the Data	✓	-
High-Performance *Computing*	✓	✓
Merging Classified and Unclassified Data	✓	

* The combination of cloud technology and artificial intelligence creates a new potential, and many AI innovations are a result of this combination. Therefore, if national security establishments will jump into the cloud revolution, the new potentials for AI innovations will become huge new

potentials.

The Infrastructure to Enable Automation

Historically, our infrastructure was built for humans. One of the big challenges to lead transformation for automation is the infrastructure. In the near future, there will be autonomous vehicles, autonomous drones, and autonomous robots. The problem in using all these autonomous machines will be the infrastructure that in the past was built for humans, and not for machines. Therefore we need to improve infrastructures such as our roads, gas stations, electromagnetic spectrum, and many others, with the view towards building foundations to enable AI automation. Nation-states that begin to address these challenges now can lead the automation field in the future. [131]

"Made in China" [132]

China decided that AI is a new paradigm for ruling the economic market as well as a core element in the competition between China and the U.S. China's vision is that AI has the potential to be a game changer that will take China into the future and lead the world. Therefore the Chinese are planning to accelerate the different fields of AI as much and as far as they can. [133] China is an example of a country that focuses on building foundations for AI with a high priority on data.

The Chinese plan includes four main efforts to develop the relevant foundations to lead the AI era. [134] The *first* step is that the Chinese government has allocated tens of billions of dollars for AI. [135] Their *second* decision is the creation of a new commission of Military-Civil Fusion that is responsible for improving the collaboration between the military and the private sectors. They understand that due to the AI era, China needs to

build a new concept of the relationship between the two sectors, including a new concept for AI acquisition. This understanding led to the creation of a new commission that is similar to DARPA (Defense Advanced Research Projects Agency), which focuses on AI and on building bridges between the military and the private. The *third* and most important decision is to leverage China's lower barriers for data collection in order to create large databases that will "feed" AI systems. [136] From their perspective, the most important asset in order to lead the concept of AI is data. China intends to collect and organize as much data as possible. According to one estimate, they are on track to possess 20% of the world's share of data by 2020, with the potential to have over 30% by 2030. This effort reflects their ambition to achieve a monopoly on data. [137]

Fourth , China decided to actively promote the idea that Chinese people should invest and work in American artificial intelligence companies. They believe that a good way to win the race between the U.S. and China is to copy American innovations, especially by Chinese working in Silicon Valley and in other AI companies and universities throughout the U.S. From China's point of view, the strongest power of AI is in the free market, and not in military organizations. Therefore they need to be inside the U.S. private sector and then bring the employees and their knowledge back home.

Acceleration

- Aggressive acceleration
- Empowering regional strength
- Automation for more and more actions
- Automation for weapons, vehicles, drones, etc.

AI Capabilities to Empower Regional Strength

The era in which human intelligence and artificial intelligence are merging enables us to choose our strongest capabilities and empower them using AI. For example, we decided to call cyber a new domain and to establish a "Cyber Command." So should we now establish an "AI Command?" Our answer is that in the near future, AI will primarily be a way to improve and empower our strongest current abilities. Therefore, a few examples for using AI to empower regional strength are (1) using AI to improve our capabilities in the cyber domain (offense and defense); (2) using AI as part of our border security; and (3) using AI to create a large amount of "targets in context." [138]

AI and Cyber

Cyber is the fourth battlefield domain (air, sea, land, and cyber). Cyberspace is a domain that enables attack and requires defense. In addition, it is a domain that enables varied types of actions to influence reality through data. Russia, China, and the U.S. have all decided that one of their main AI efforts will be to increase cyberspace capabilities. Their decisions include using AI to improve the ability to build cyber-attack tools; to improve defense capabilities to find new viruses; and to enable attackers to find relevant files in their rivals' and enemies' networks. [139] For example, China is developing a department of AI tools for cyber-defense and cyber-attack. They believe that cyber is a strong domain in China and that AI is a relevant innovation that can empower their cyber capabilities. As a result, China decided to establish a new unit that will focus on cyber and AI to enable the acceleration of this specific new ability. [140]

Machine-Learning and Cyberspace – A Case Study

In cyberspace, there are myriad viruses and cyber-attack tools that can act

against your network. [141] There is no option to "clean" your network of viruses. Viruses mutate all of the time, and viruses create new viruses. In addition, there are people and computers that want to attack your network for different reasons. [142] One of the challenges is that even when a cyber-attack tool is caught, it is still possible for the cyber-attacker to alter this tool a bit and to use the new version of the virus to attack again. For that reason, we don't have any choice in cyberspace. We are required to deal with viruses and cyber-attack tools 24/7. The mission is not to clean the network, but rather to build our network with the ability to "live" with some viruses and to choose which of them we need to totally destroy. [143]

Recruiting Effort for Machine-learning to Solve the Problem

Machine-learning has the potential to deal with infinite data; it can even identify cyber-attack tools from big, known data and discover new cyber-attack tools that were previously unknown. Additionally, it can learn through past viruses how to discover potential new viruses. Machine-learning also has the potential to make predictions about new viruses and new cyber-attack tools in a way that a human brain cannot do alone. As we discussed, there are three main floors that are required to build machine-learning to solve this problem: (1) we need data to build a model to suggest the new viruses or new cyber-attack tools; (2) training and tuning to improve the model; and (3) making predictions and using the model to improve our defense in cyberspace. It is important to realize that machine-learning can also help cyber attackers create new viruses that will be difficult to detect.

The First Floor – Data to Create a Model

The first floor is data to build a model. The basis for machine-learning in

this case is data regarding viruses and cyber-attack tools from the past. The data needs to be as big and as varied as possible, including data about the viruses, their characteristics, the ways they try to "hide," and so on. When we have enough data, we need to prepare and organize it in a manner that allows the machine to work with it, including the servers, the way in which the information is stored, and the ability to link between different parts of the information. The last step for this section is building a model. For example, a file or code that looks like "x" has great potential to be a new virus. Building a real model is both complicated and challenging.

There are at least two ways to build the concept for a model. We may choose strong features, and if these features exist, there is a good possibility that there is a new virus. Another option is building a model that is based on a quantity of features (hundreds or even thousands). This model will be robust because of the quantity and variety of features. The best option is to build the model with a few strong features as well as with a large number of varied features. A robust model should be created through a "control group" of viruses that we know for certain are dangerous.

The Second Floor – Training and Tuning

Once we have the model of the suspect viruses, we can begin training. We can take the model and start to check it again with the data. The training will help improve the machine, check if the features work, and find the relevant suspicious viruses. During training we can improve the preciseness of the model. For example, the model might give more priority to "shape patterns" [144] than to other features, and because of this focus, there is the potential for mistakes. With training, we can make small changes to a few parts of the focus or to the priorities of the model. When we finish training, we have an improved model. Then with the data and the best model, we can apply it to the real world and check this model with new data and see

the results.

Third Floor – Evaluation and Prediction

This is the time for evaluation. We can use real data and real experiences, like the machine-learning is going to encounter at the end of the process. For our example, we can use the model to discover new viruses with new data. The end of this step is the option for hyperparameter tuning. For example, if during the evaluation we see that one feature is stronger than the others, we can decide to give it more priority. Now, when we have data and the improved model, we can go to the last and final step of prediction – putting the model on the machine – and the machine can begin to identify and suggest viruses and cyber-attack tools.

Borders with an "AI Wall"

Defending our nations' borders is a challenge that has become more and more complicated. The wall between the U.S. and Mexico, and the underground tunnels that Israel faces along its borders with Gaza and Lebanon, are just a few examples of these challenges.

The Human-Machine Team enables a new potential to use AI to build a "smart area" for protecting borders. The ability to connect various bits around the border through machine- learning can help control these areas and protect the borders. The smart area is required to define the location, to organize the relevant sensors in the context of the operational problem, and to prepare the "channels" of the information in the context of that same location. In addition, we must organize a team to utilize the information of the "smart space." All of these factors together can achieve an improved operational response. When we implement this concept, we will succeed in building an "AI Wall" to empower our efforts and improve

security along our borders.

Russia and the Idea of Acceleration

We have already mentioned President Vladimir Putin's "AI is the future. AI is the future not only for Russia, but for all humankind…whoever becomes the leader of this sphere becomes the ruler of the world." This was a signal to several sectors in Russia (including the government, universities, industry, and the general population) to focus on the field of artificial intelligence. From the Russian perspective, AI is a main area to help the digitization of their economy. In addition, military power is an aspect of Russia's grand strategy, so AI is also a part of its warfare planning. Traditionally, Russia has had challenges in taking their amazing ideas from concept to the development of real, new technologies. They are trying to change this basic situation with an internal focus on artificial intelligence. [145]

The Russian vision for the next few years is to realize Putin's resounding words by *accelerating* the capabilities of AI in Russia. Their ambitions are to *empower the self-respect* of the Russian people, to *improve their economic situation* and *GDP* , to *reverse the technological brain drain* from Russia to places like Silicon Valley in the U.S., and to build *control systems* based on AI. In addition, they want to develop AI as a relevant *strategic tool* to address allies such as China, and as part of their efforts against rivals and enemies. For example, in its efforts in Syria, Russia takes more and more steps to improve its military capabilities in the arena by using artificial intelligence.

How Does Russia Plan to Realize Its AI Vision?

In order to achieve these goals, Russia has built a *road map* that includes five core steps. The main concept is to take specific issues and accelerate

them by using AI. For them, acceleration means achieving new abilities as fast as they can, and forcing the nation and organizations to improve their foundations to enable this acceleration. *First* , Russia decided to build AI capabilities to empower their regional strength. This means developing AI in their propaganda, in their "fake news" efforts, and in the electromagnetic spectrum, and as part of cyberspace. *Second* , they decided to focus on robotics and automation, including the automation of large vehicles such as tanks. The goal that the Military Industrial Committee set is to succeed in achieving a reality in which 30% of Russian military equipment will be robotic and autonomous by 2025. *Third* , to support these transformations, Russia is investing hundreds of millions of dollars, [146] and they are developing new, professional AI departments in universities and institutes in Russia. In addition, they decided to create a defense research organization, roughly equivalent to DARPA, dedicated to autonomation and robotics, called the Foundation for Advanced Studies. *Finally,* they are trying to improve the relationships between national organizations and the private sector to help keep the Russian "brains" inside of Russia. [147] For example, Kryptonite is a Russian company that works on creating "civilian IT products based on military developments in information security, including blockchain." Specifically, Kryptonite's work involves "cryptography, machine-learning, big data, quantum computing, blockchain, and the security of telecommunications standards." [148]

"Singularity Time"

Singularity time is thinking and establishing places (departments, units, organizations, and companies) that will focus on the distant future and on ideas that today seem totally unrealistic. [149] It also implies starting to build our organizations using concepts from the family of general AI (and not only from narrow AI). As previously discussed, general AI – sometimes

called Artificial General Intelligence, or AGI – is a machine that can replace an entire human being, or at least has the level of cognition that is equivalent to that of a human. General AI refers to a notional future with an AI system that exhibits intelligent behavior, feelings, and context at least as advanced as a person, across the full range of cognitive tasks. General AI is in contrast to narrow AI, which refers to specific capabilities and not to the whole system.

The purpose of this idea is to prepare ourselves for the future and to help discover ideas from the future that will also enable the current acceleration of AI. Moreover, this concept includes the necessity of building basic infrastructure foundations, such as roads and highways, that will facilitate the use of autonomous vehicles.

Next Generation Unit

"Good morning, car. Please take me to my office." This is an AI reality that can be achieved in the near future. The day the car answers, "No, I decided not to drive you today" will be a singularity moment. The situation where one morning a machine will decide to attack a target "for its own reasons" is an example of a singularity moment. In this example, the AI machine has intelligent behavior, feelings, and context that are at least as advanced as a person's, across the full range of cognitive tasks.

We cannot imagine the future of AI in 2040, 2050, or beyond. Personally, I believe that the concept of a self-aware "Terminator" robot is unrealistic and will not be part of our lives. However, today it is important to establish a unit in national security establishments whose responsibility is to build tools for the distant future. This pioneering effort will help us take responsibility for the future, create the future, and be prepared if such a singularity time does arrive. Finally, the unit will have the option to dream without limits, which will help broaden today's narrow AI capabilities.

One way to take responsibility for the future is with "singularity time labs." The idea of these labs refers to establishing new labs with the idea of focusing on the distant future and on concepts that today seem totally unrealistic. Culturally, the labs need to be under the umbrella of a few big universities; in addition, there need to be government labs, financed by government bodies such as the Department of Defense, and at the same time have environments similar to and connections with new startups.

---

123 2018 DoD Artificial Intelligence Strategy: "*Harnessing AI to Advance Our Security and Prosperity* " (February, 2019), 1-4.

124 *GPU server* is a technology innovation to deal with a great amount of data and to enable high-performance computing. This "super-computer" enables multiple actions at the same time and in parallel. Therefore, this is a revolution that is a base for innovations that need big data, such as machine-learning.

125 The idea of "singularity time" is discussed at length in Kurzweil's books. Specifically, see Ray Kurzweil, *The Singularity Is Near* (city? Penguin Books, 2005), 123-128.

126 Thomas W. Malone. op. cit., 269-272.

127 Stuart J. Russell, Peter Norving, op. cit., 1062-1063; Paul R. Daugherty, James H. Wilson, op. cit. , 208-211.

128 Ajay Agrawal, Joshua Gans and Avi Goldfarb. op. cit., 11-20.

129 Ajay Agrawal, Joshua Gans and Avi Goldfarb. op. cit., 188-189.

130 *GPU server* is a technology innovation to deal with a great amount of data and to enable high-performance computing. This "supercomputer" enables multiple actions at the same time and in parallel. Therefore, this is a revolution that is a base for innovations that need big data like machine-learning. You can just write "see end note # 126.

131 On the other hand, when we build new automations, we need to ensure that these innovations can be based on the same foundations that were built for humans.

132 Paul Mozur. "Beijing Wants A.I. to Be Made in China by 2030." *New York Times* , July 20, 2017, https://www.nytimes.com/2017/07/20/business/china-artificial-intelligence.html

133 Ajay Agrawal, Joshua Gans and Avi Goldfarb. op. cit., 218-220.

134 Congressional Research Service on *"Artificial Intelligence and National Security"* (April, 2018), 17-21.

135 This step is similar to the Chinese strategy of making large investments in emerging technologies and leading the world market.

136 Ajay Agrawal, Joshua Gans and Avi Goldfarb. op. cit., 218; Congressional Research Service on " *Artificial Intelligence and National Security*" (April, 2018), 17.

137 Gregory C. Allen. "Understanding China's AI Strategy," Center for a New American Security, February 6, 2019, https://www.cnas. org/publications/reports/understanding-chinas-ai-strategy ; Congressional Research Service on *"Artificial Intelligence and National Security*" (April, 2018), 218-220.

138 Chapter 3: National Security in Between Paradigms, new opportunities.

139 Congressional Research Service on *"Artificial Intelligence and National Security"* (April, 2018), 10.
140 Congressional Research Service, op. cit., 17-21.
141 Cyber-attack tools refer to viruses that are specifically created to penetrate a network and hack against this network. hack it?
142 Executive Office of the President National Science and Technology Council Committee on Technology. op. cit. , 36-3 ??? 36-43?
143 Congressional Research Service. op. cit., 10.
144 "Shape patterns" are features that are based on the structure of the algorithms.
145 Congressional Research Service, op. cit., 21-22.
146 In comparison to China and the U.S., this is not a lot of money to invest in this field, but for Russia, in rubles, this is a significant budget.
147 Samuel Bendett, "In AI, Russia Is Hustling to Catch Up." *Defense One* , 04 April 2018. https://www.defenseone.com/ideas/2018/04/russia-races-forward-ai-development /147178/ ; Bendett, Samuel, "Here's How the Russian Military Is Organizing to Develop AI" in *Defense One* 20 July 2018. https://www.defenseone.com/ideas/2018/07/russian-militarys-ai- developmentroadmap/149900/
148 https://caai.blog/2018/07/18/russian-kryptonite-to-western-hi-tech-dominance/
149 The idea of "singularity time" is widely discussed in Kurzweil's books. Specifically, see Ray Kurzweil, *"The Singularity Is Near"* (Penguin Books, 2005) 123-128. I suggest just writing "See end note #127."

CHAPTER 6

What We Can Learn from the United States about Leading AI Transformation[150]

Artificial intelligence has been hyped in the U.S. innovation system. [151] From the Americans' perspective, AI is one of the main catalysts for innovation today. The U.S. has a relevant culture and a good system of innovation to continue to lead emerging world technologies. At the beginning of 2019, the White House unveiled a national AI initiative; the plan focuses on the relationship among industry, the education system, regulation, policy, the military and the government. [152]

On the one hand, it is difficult to figure out the U.S. strategy for AI and exactly what the plan is to take it to the era of AI. On the other hand, all the countries that have strategies for AI want to learn from the U.S., and they are striving to join U.S. companies. "Culture eats strategy for breakfast," [153] and the U.S. has a culture of innovation. At present, the largest and strongest digital companies that are developing AI are in the U.S. Therefore, it is very important to answer the question "How is the U.S. preparing and building itself for the AI revolution, and what can we learn from the process?"

"We Have No Choice"

"We have no choice." This is the first thing I heard from several leaders in the U.S. China and Russia are accelerating their AI capabilities, and the U.S. has no choice but to forge ahead and lead the field. For example, China, which is widely considered to be the biggest threat to American technological leadership, released a plan in July 2017 for dominating the

global AI market. Allies like France, Canada, and the U.K. have also unveiled their own national AI strategies. Consequently, the U.S. has no choice but to be the world leader in AI transformation. [154]

In addition, national and economic leaders believe that AI is not just a temporary buzzword, but think that it is a serious issue with significant potential. They look at AI as the current engine for their innovation system, yet at the same time recognize that its development is decentralized and a challenge to coordinate. Finally, these U.S. leaders understand that there must be partnerships between government and the private sector, as well as with allies, in order to succeed on the AI journey. [155]

A Systematic Process

One of the decisions that U.S. leaders are discussing is building a systematic process for AI, that would include maintaining a constant status report about the development of AI in relevant agencies and organizations. In addition, they are planning to build a pipeline for AI development that includes universities, industry, the workforce, and others. They decided that every agency and organization needs to build its own AI strategy, and that the government needs to build centers to help increase the speed of the processes and make them successful. From the budgetary perspective, the U.S. decided that first of all, every governmental organization needs to allocate part of its budget for AI and to report on how much it is and what it is for. In the coming years, the government will increase the overall budget for AI. The U.S. recognizes that it must increase AI resources every year, including budget, research and development, and the workforce. For example, DARPA committed $2 billion to explore state-of-the-art AI applications over the next five years; overall, the U.S. government plans to develop AI systematically. [156]

The Main Idea of the American Plan for AI

The two important words needed to understand the U.S.'s plan are *accelerate* and *harness* . The first idea is to accelerate AI capabilities and to accelerate the real potentials for AI. This means that the future will have different types of AI capabilities, and the government's responsibility is to accelerate and facilitate the process and continue to lead this field. The second is to harness the capabilities of AI to improve national defense, which means that the government is responsible for discovering where, when, and how AI can help national defense missions and then to make them happen. [157]

The Key Principles for Leading AI Transformation Experimentation

The *first* step of AI transformation is experimentation. The idea is to choose a few specific missions that AI can help now, and to build AI projects for them. It is important to note that the U.S. leaders believe that when developing AI, they must embrace risks and accept failures. They understand that in the field of AI, the best way to improve is through experimentation; therefore, early failures on a small scale are required for overall success and for the acceleration of AI. This concept goes against traditional U.S. military and governmental culture, in which the desire is to check the conditions and act only when conditions are secure and safe, and when success is certain. However, when it comes to AI development, the Americans realize that it is essential to take risks and experience multiple small failures in order to succeed in the larger process of AI transformation. It seems that in the field of AI, the U.S. has chosen a strategy similar to that of a hi-tech entrepreneurial company. [158]

The Foundation

The *second* step of AI transformation is building a basic common foundation. AI projects need data, a way to keep and organize it, and powerful computing to handle the quantity of the data. Traditionally, national organizations are lacking in all of these fields, and a common foundation and infrastructure are crucial. The foundation includes an idea about how to build a field of 2,000 GPU servers, [159] a project to help use industry clouds for national security, and an effort to improve the culture of sharing data. The bottom line is that the current foundation needs improvements to enable the AI Revolution. The first improvement that must be made is the ability to find the relevant data, including "government data," and the ability to use it (an important key to achieving this goal is data regulation). [160]

Collaborations and Bridges

Strengthening the Bridges between National Security, Academia, and the Private Sector

Historically, the U.S. has leveraged close relationships between defense, academia, industry, and the private sector. For example, DARPA is a unique organization whose mission is to build bridges between government, academia, and industry, and to constantly strengthen these connections. The Department of Defense is also responsible for building these relationships and constantly improving them, by relevant acquisitions and projects.

The *third* decision of the U.S. is that AI requires new collaborations between the military, industry, and academia. In addition, AI transformation also requires new collaborations with allied countries. These collaborations need to be synergistic, to enable new capability leaps, and to enable engagement and evolution. Moreover, America's leaders are looking for potential opportunities to merge research and operations to fulfill

specific missions, as well as to learn from these experiences. Ultimately, the leaders want a circular innovation system in which government will empower the private sector; after that, the private sector will empower the government, the national security establishments, and the economic situation. This circular innovation system will continue to mutually empower every component going forward into the future. This is the ideal innovation system, and currently the U.S. is implementing AI as a part of it.

Consequently, the U.S. decided that DARPA, DNI (Directory of National Intelligence) and other government establishments are required to develop the next generation of collaboration to introduce the technologies of Silicon Valley into the military. This revolution includes the ability to share successes, failures, talented people, data, and so on. In addition, it requires a new concept for acquisition, and partnership with academia, as well as for using these bridges to build data centers, new labs, and new capabilities. [161]

Laws and Ethics

The *fourth* step is to build the system of laws and ethics to address these new capabilities. Nowadays, Google knows much, much more about all of us than Stalin ever knew about his people. Without a system of laws and ethics, AI has the potential to undermine freedom. One of the Western world's challenges is China's and Russia's declaration that they want to be a part of this system of laws and ethics. However, they know that such a system will create problems for the U.S., China and Russia can potentially sign onto this new AI legal system and then continue to do whatever they want without following the new rules. [162]

"The Joint AI Center (JAIC)" – A New Heart for AI

In 2016, the U.S. Defense Innovation Board, chaired by Eric Schmidt,

recommended the creation of an AI and Machine-Learning Center of Excellence inside the Department of Defense to spur innovation and transformational change. He added that an organization of this type could also create a single focal point for Congress to consult on defense-related AI issues. The *fifth* step is implementing this recommendation. AI development is currently supervised by a new DoD unit, the Joint AI Center (JAIC). This decision is meant to build a unique system to help accelerate AI capabilities and concepts. The JAIC is headed by a three-star general; its purpose is to address the complicated situation, enable the partnerships outside the military, and accelerate and lead the AI Revolution. [163]

AI and Cyber

The *sixth* step is to focus on AI and cybersecurity. From the American perspective, it goes both ways: AI helps cybersecurity and cybersecurity can help AI. Therefore, the U.S. military organizations need to focus on the relationship between cyber and AI; this includes using AI to improve the ability of analysts to deal with infinite data from cyber. An example is using speech-to-text and machines to figure out unique details from databases. In addition, it includes a plan to use AI to improve both defensive and offensive cyberspace capabilities. [164]

The U.S. and the Concept of FAST – A Comparative Analysis

Basically, the American plan for AI deals with the main characteristics of Foundations, Acceleration, and Singularity Time. However, to empower their plan, I recommend paying attention to a few issues that have not received any unique focus:

- Creating a "closed-open-closed" network to address and merge classified and unclassified data
- Learning from China and building strategy for leading "world data"
- Creating the "data roads" between various organizations, networks and clouds.
- Acceleration for a few specific big issues (and not as many acceleration projects as possible).
- Empowering the relationships between government and big data companies (Google, Amazon, Microsoft, and IBM) and making these relationships similar to the relationships between the government and companies such as Boeing and Lockheed Martin.

---

150 Today, the U.S. leads the innovation system globally. There are hundreds of references for this section. Some of them are from meetings, readings, and discussions during my studies at the National Defense University, and some are from meetings with members of the NSA, DARPA, and the DoD and other organizations. In the literature review, there is a section on the three articles that were most helpful to me when putting this section together.

151 Innovation system is a concept to describe the unique relationship in the U.S. between the government, industry, the private sector, and academic institutions that lead to innovations.

152 2018 DoD Artificial Intelligence Strategy: *Harnessing AI to Advance Our Security and Prosperity* (February, 2019), 5.

153 It is a well-known idea coined by Peter Ferdinand Drucker. Drucker was an Austrian-born American management consultant, educator, and author, whose writings contributed to the philosophical and practical foundations of the modern business corporation . He has been described as "the founder of modern management."

154 2018 DoD Artificial Intelligence Strategy: *Harnessing AI to Advance Our Security and Prosperity* (February, 2019), 5. (I suggest just writing "See end note #154."

155 Executive Office of the President National Science and Technology Council Committee on Technology. op. cit., 3-4.

156 Congressional Research Service, op. cit., 17.

157 2018 DoD Artificial Intelligence Strategy. op. cit., 5, 17.

158 2018 DoD Artificial Intelligence Strategy, op. cit. ,1, 4, 7.

159 *GPU server* is a technology innovation to deal with a great amount of data and to enable high-performance computing. This "super computer" enables multiple actions at the same time and in parallel. Therefore, this is a revolution that is a base for innovations that need big data like machine-learning. You can just write "see end note # 126.

160 2018 DoD Artificial Intelligence Strategy, op. cit., 2.

161 2018 DoD Artificial Intelligence Strategy, op. cit., 16.

162 Executive Office of the President National Science and Technology Council Committee on Technology, op. cit., 2-3.
163 2018 DoD Artificial Intelligence Strategy, op. cit., 9-10.
164 Congressional Research Service, op. cit., 10.

PART 3

Plan of Action

A Framework and Principles for the Plan

The Top 5:

1. Building data centers
2. Developing an innovation system+
3. Structures and functions that can support FAST transformation
4. Accelerating the acceleration
5. FAST for enabling MDO (multi-domain operation)

4 x 4: A Powerful Management Tool and the Required Leadership

Epilogue and Personal Notes

CHAPTER 7

A Framework and Principles for the Plan

A Goal without a Plan Is Just a Wish [165]

"Don't talk to me about the 'what.' Talk to me first of all about the 'how.'" From my experience, to lead AI transformation, the "how" is much more important and more consequential than the "what." Furthermore, the organization as a whole must undergo transformation. The missions change, processing bodies change, there are new positions and structures, and so on. "Context" is a magic word. The secret to success (or lack of it) lies in the ability to build up power in the relevant context. A plan of action for leading The Human-Machine Team transformation requires functions that will manage the relationship between the previous paradigm and our generation. [166]

Can We Grow into the Future and Lead Transformation without Crisis ?

As we discussed in the introduction, Thomas Kuhn, in his *The Structure of Scientific Revolutions* , maintains that the great revolutions of humanity grew from crises. Kuhn views the periods in between paradigms as "crisis periods" that usually emerge as such only in retrospect. Hence, when it comes to digital transformation, there is no need to fear clarifying the situation and pointing to the current crisis because, obviously, without crisis there will be no revolution. Until we formulate and define which crises each of our organizations have failed to provide responses for, we cannot begin transformation. However, the new potentials of The Human-Machine Team need to be strong enough to force transformations on our organizations. In addition, national security organizations have long been

accustomed to being at the forefront of emerging technologies, but when it comes to AI, the private sector is way ahead. [167] Acknowledging this gap could be a motivating factor to help national security organizations grow into the future and lead transformation without crises.

In Praise of Ontology

Ontology is a complex philosophical issue. When we talk about AI and digital transformation, the main points that we need to take away are the relationships between different types of data. Ontology was born long before the digital era. It is the theory of "what is," of existence, and it poses questions about the various entities that exist in the world and the network of connections between them. Ontology deals with things that are shared, with what causes them to exist, and with what causes them to be connected.

In the Information Age, clarifying, defining, and conceptualizing ontology is important. Information includes different entities that have a network of connections between them. A main precondition and key to success in organizing the data is defining the ontology of the information. These connections between the different types of data (ontology) are the basis for guiding the organization's digital transformation. For defense establishments, the basic ontology concerns the network of relationships and links between the person and the place. [168]

For example, when targeting the enemy, one first seeks to mark the location and then focus on the people there. It is the relationship between places and people – in this exact order. Another example of ontology is a way of organizing data in order to thwart terror attacks. In this case, the point of departure is often a person (who may want to perpetrate a terror attack), and following that, we try to locate him. In this example, the relationship is between people and places in this exact order (i.e., people

first). Ontology, of course, involves additional and complex levels of relationships and links between the entities (different objects, additional people, other places, fields of activity, etc.). Without a precise definition of ontology, one cannot craft a strategy and an architecture for information. [169]

Acceleration: Big Enough and Small Enough; Foundations: As Wide as We Can

Machines can learn from experiences, and the best way is to learn from experimentation. Therefore, to accelerate the development of AI, we need more and more experimentation. At every moment, every organization needs to be conducting at least three to four AI experiments. We need to learn from AI successes as well as from failures, and to systematically improve our machine-learning and our organizations. The concept is to choose steps that will be both big enough and small enough: big enough to be relevant, and small enough to successfully contain the first new steps. Again, the idea is to increase the pace of development and help achieve acceleration. However, when we talk about foundations, they need to be as wide as possible. Foundations can improve the current situation and, more importantly, they are the required conditions to fulfill the potentials of AI. [170]

The Human-Machine Team: The Next Generation of Moore's Law

Moore's Law, a term coined 50 years ago, is the observation that the number of transistors in a dense circuit *doubles* about every two years. It is named for Gordon Moore , the co-founder of Fairchild Semiconductor and CEO of Intel . In 1965, his paper described a doubling in the number of components per integrated circuit every two year s, and projected that this rate of growth would continue for at least another decade. It is amazing to

see that this is still relevant today, especially regarding automation. In other words, with each passing year, every organization, every unit, and every nation should strive to double the functions that are automated by AI machines. Since automation involves such a wide spectrum, we can and we should use Moore's Law as a metaphor for a model of how to increase the pace of partial and full automations year after year. [171] Moreover, the concept of The Human-Machine Team ("super- cognition") has the potential to be the next generation of Moore's Law.

Resources and Efforts

In the next few years, we will need money and "brains" invested in AI to take us to the future. How much money, and how many brains, depends on the mission and also differs from one organization to another. However, the resources need to be related. Artificial intelligence first of all will improve traditional capabilities and traditional missions, and therefore these investments can be made using internal resources. When someone goes to a psychologist, the fact that he pays $200 an hour is of value, and it requires him to assume part of the responsibility for the treatment's success. Similarly, organizations need to understand that AI is a core requirement to improve their missions, and the requisite funds must be found inside their current budgets. We have no choice: It is our responsibility, and we cannot wait for additional outside funding. [172]

---

165 Antoine Marie Jean-Baptiste Roger was a French writer, poet, aristocrat, journalist, and pioneering aviator.

166 Paul R. Daugherty, James H. Wilson, op. cit., 175-176.

167 You can see the following chapter about "Innovation System+". ??? Please give the number of the chapter (and maybe even the page).

168 Maj A., "Analyzing Network Intelligence in the Big-Data Era: Intelligence in Theory and in Practice. "*Big Data and Intelligence*" (a journal on Intelligence Methodology, October 2018), 54-61.

169 Col. Y, "Intelligence in Theory and in Practice." *Big Data And Intelligence* (a journal on Intelligence Methodology, October 2018), 16-17.

170 2018 DoD *Artificial Intelligence Strategy* , op. cit., 1-3.
171 Moore referred to a physical, technical phenomenon, and here I use it for a metaphor of "process." (Please make sure that this is correct.)
172 Executive Office of the President National Science and Technology Council Committee on Technology, op. cit., 25-26.

CHAPTER 8

The Top 5

The Plan of Action needs to be organized with three main efforts. First is the "data effort," to acquire more and more data and organize it. Second, a "cloud effort," to effectively use and maximize all the potentials of cloud technology. Third, the "acceleration effort," to choose specific missions that can be accelerated by AI and update organizations to accomplish these missions.

1. Data Centers

Data Centers, Data Scientists, Data Analysts, Data Data

I have chosen to begin the main chapter of this book with the word "Data." At the end of the journey we can say, "Tell me what your data is and I'll tell you your potential for successfully completing your mission." Therefore, every nation, every organization, and every department needs people and resources focusing on data (tagging, organizing, cleaning, and storing it). For this we need to build data centers in every country and every organization, and we need data scientists and data analysts. "Tell me your data and I'll tell you your potential." [173]

The National Data Carrier (NDC)

Traditionally, governments are responsible for building national water carriers. Water is a basic requirement for all humans, and so the governments must meet this need and enable water to be distributed to the people. Since the dawn of time, water has been the basis for the existence

of humankind. During the Agricultural Revolution, people developed ways to bring water to their villages, and during the Industrial Revolution, nations built water carriers across and between nations to bring this vital resource to their populations. During the Industrial Revolution, petroleum and coal were two resources that enabled the innovations during that period. Hence, governments developed the infrastructures for transporting fossil fuel products from place to place and to use it all over their countries.

"Data is the new oil," and data is the basis and foundation for the Digital Era; this means that innovation and success in the DE are dependent on the data. [174] Therefore today, governments need to build "national data carriers" (NDC). Governments need to provide academia, industry, and the private sector, as well as their entire populations, with as much data, as varied data, and as organized data as possible. Governments that build national data carriers will provide their populace, companies, and academia with a huge advantage. An innovation system and innovation ecosystem is first of all based on data for the system. Moreover, the data carriers will be a new opportunity for governments to build relationships with Google, Amazon, Microsoft, IBM, and others in ways similar to their current relationships with companies such as Lockheed Martin and Boeing. An NDC has the potential to be the tipping point and game changer in the competition between nations and between organizations. [175]

2. Innovation System+

One of the magic properties of U.S. strategy is the bridges between the government, academia, and industry that create the U.S. innovation system. One of the ways this circular system is enabled is by the small players who help function together with synergy to strengthen the whole system and to empower each player. Examples of these small players are government labs, DARPA (Defense Advanced Research Projects Agency),

DIU (Depart of Defense Innovation Unit), and IARPA (Intelligence Advanced Research Projects Activity).

The *government* enables and generates this system, which means that it invests the initial capital, establishes policy that enables the innovation system, and takes care of the system as a whole. *Academia* is located at the center of the knowledge and at the center of the creativity that accelerates the system; it is also the place to ask complicated questions and lead innovation without limits and without the requirement to monetize. Interestingly, innovation hub systems are located around prominent universities (Boston with Harvard and MIT, San Francisco with Stanford and Berkeley, and even smaller cities such as Pittsburgh with the University of Pittsburgh and Carnegie Mellon). *Industry* and the *free market* have the responsibility in the process to take good ideas to the real world and lead creativity for systematic solutions. Industry and the free market also need to monetize these innovations.

Small players empower the bigger ones and help the circulating nature of the system. A good way to help the system innovate is through the mutual capabilities of two or three big players acting together in one small organization. These players have one foot in the academic world and the other foot in industry, or else they have one foot in government and the other in the free market, and so on. An interesting example is DARPA, an agency of the U.S. Department of Defense (DoD) that is responsible for the development of emerging technologies for use by the U.S. military. It is a small organization, with only about 240 employees, of whom more than 100 are product managers – and a budget of $3 billion. Most of its employees are professors from academia who work for DARPA for four years as leaders of a technology project. The projects help the military to address their missions, and support industry and the private sector to earn their profits. DARPA uses government money and invests it in academia, in

industry, and in the private sector. We can look at DARPA as critical oil on the chain that helps the whole system run better and faster. This small organization makes a significant contribution to the U.S. innovation system.

In order to lead success in AI, we need to strengthen these kinds of bridges, build new bridges, and build them with a simple process to influence each other. For example, in the cyber domain, the bridges with industry are relevant, but the strongest cyber company is still the NSA (National Security Agency). In the field of AI, the best companies are in private industry (in Silicon Valley, for example), and so we must build bridges between the private sector and the government to strengthen each other. The national security organizations don't need to be "No. 1" in AI, but rather they need to be "No. 1" in using AI capabilities to meet their challenges and accomplish their missions. Today, the competition of AI is a competition to lead the innovation system globally.

The "Secrets" of the U .S. Innovation System

One "secret" of the U.S. innovation system and the environment that enables this ecosystem is that each player becomes stronger as a result of being a component of the whole system. At the same time, the entire system is strengthened by the participation of all the players. Here, the classic saying is true – that the system is greater than the sum of its parts. It is a win-win system called "The Triple Helix. " "One foot here, and one foot there" is a unique characteristic of the Triple Helix. This means, for example, that there are professors in academia who spend part of their time working for companies in industry and the private sector, and managers who have positions in different fields at the same time. Another example is the labs in academia that get their budgets from the military to create new technology for the military. Moreover, the government invests money in academia, academia works with industry and with the government, and

industry is highly focused on government organizations.

The second "secret" is the process. There are superpowers like China, with strong markets; countries like Russia, with good universities; countries like Saudi Arabia that invest a lot of money in their militaries; and countries like Israel, with "startup cultures." The strength of the innovation system in the U.S. is the process, which is strong and systematic, and enables all these fields and all these players to act together like a team.

The third characteristic is the high priority placed on research and development. This means that resources are allocated for R&D (for labs, institutes, academia, industry and government organizations). It is important to note that there are also many R&D centers in different countries that participate in the U.S. innovation system, thereby enabling the system to benefit from other ideas, cultures, and brains.

Finally, and most importantly, the American culture of innovation is paired with a culture of working within a system. This means a culture of defining problems and developing solutions; the "American Dream" – that if you work hard you can achieve just about anything; thinking about issues on a large scale; long-term planning; and embracing processes and systems. Together, these cultural characteristics enable the U.S. to build an innovation ecosystem not only in big cities and big locations, but also in small cities and small locations.

For example, in Pittsburgh there is a budget from the State of Pennsylvania to build a startup incubator. This incubator has strong ties to the University of Pittsburgh. The ecosystem in Pittsburgh collaborates with the military and focuses on innovations in robotics – it is an example of the circular innovation system. In this case, the government empowers the private sector, then the private sector empowers national security establishments, and the local economic situation improves as well. Moreover, the circular innovation system continues to mutually empower

every element going forward into the future. The bottom line is that the U.S. innovation system is not just collaboration or close relationships, it is a "win-win" system with a culture of working within a process and a culture of innovation. [176]

The Unique Challenges for the Innovation System in the AI Era

Traditionally, national security establishments have known how to lead procurement systems and innovation systems. As we discussed, over the last few centuries, security establishments used to be the "No. 1" inventor and developer of weapons and military capabilities. For example, the U.S. Air Force is also the power behind the acceleration of airplanes for use in the private sector. The best airplane is always an Air Force plane. Moreover, companies like Lockheed Martin are a kind of "inside ability," because even though they are part of industry, the company, in essence, is part of the U.S. national security system. Therefore, operating the acquisition system with companies like this is much easier.

Today, the opposite is true in the field of AI. The free market and private industry have many more resources than anyone else, and they lead the field of AI. National agencies and national organizations do not know how to deal with the new AI reality. In addition, national establishments know how to buy and lead acquisition for hardware capabilities, yet in the AI field, the innovation system requires the organization to also lead acquisition and innovation in software. This is a cultural challenge for national security establishments. [177]

Innovation System+ (An Innovation System to Lead FAST)

"We don't have one strategy; we have a system and an ecosystem." This refers to the strength of the system and the ecosystem of innovation in the

U.S. Moreover, it refers to a system that became a growth engine for technology and economic prosperity, and leads the world's innovation systems. Today, the competition for AI is a competition to lead the innovation system globally. To be a leader in AI, a nation needs to create the "Innovation System+." [178] This refers to strengthening the bridges and empowering the connections between government, industry and academia to fulfill the idea of FAST and harness the AI era. The traditional innovation system helps the military to empower hardware capabilities such as vehicles, planes, and weapons. The Innovation System+ will empower military operations by bringing in the software capabilities of AI. The challenge is that AI is scattered among industry players (including many small companies). The Innovation System+ can lead the next generation and the next revolution of the Digital Era.

3. Structures and Functions that Can Support FAST Transformation

A structural perspective is a key factor in leading organizations to the future. Structural changes are a basis for relevant transformation. One of the complicated and unique challenges that security establishments have is to lead transformation, yet be prepared for war at the same time. How can the security establishments reach the next high-level paradigm and at the same time be prepared to achieve victory in wars that are operating in the previous paradigm? In other words, one of the main characteristics of a military organization is the responsibility to be prepared for war at all times, 24/7. The possibility of a war breaking out at any given moment makes preparedness the top priority. [179] It is very difficult to dream of innovation, to carry out the transformation, and to improve preparedness in the same organization with the same resources.

Therefore, a new national security establishment structure is required to go forward and at the same time maintain preparedness by using

traditional capabilities. In addition, one of the structural challenges is to decide when to build a new unit, section, or organization, and when to keep the same unit and the same structure, and just change issues inside the organization.

Structures to Support the Idea of Innovation System+

As we discussed, "small players" have the potential to make acceleration happen. The idea of aggressive acceleration refers to our responsibility to accelerate the process and bring the future to the present. Small players, who have the ability to empower the big players and help the circulating nature of the system, can make it happen. Therefore, every specific idea to accelerate AI capabilities needs to have an organization (a small player) whose responsibility is to lead this "acceleration mission." For example, if you want to build a "smart border," it is advantageous to first establish a new unit (small player) in an organization that focuses solely on this mission. Likewise, if you want to accelerate the utilization of drones with AI capabilities (e.g., a swarm), you should establish a new unit for this purpose.

These new small units (players) must have mutual capabilities of two or three different big players (government, academia, and industry). For this they need to have "one foot here, and one foot there" and operate together in a specific, small organization. Every acceleration mission should be led by a related small player. In addition, due to the unique challenges for the innovation system in the AI era, government organizations like the DoD need to build related sections that will have professionals trained in how to merge AI capabilities into government bodies. On the other side, AI companies and "data superpowers" like Amazon, Google, Microsoft, and IBM need sections or units with a focus on merging with government organizations.

Building New Digital Units Based on AI (to Accelerate the Pace)

National security organizations should establish new units that specialize in big data and data science and are based on merging between human intelligence and artificial intelligence. There are at least three reasons that it is so important to build these new units: (1) they have the potential to be more focused, and have more knowledge and ambition to achieve success based on AI; (2) they can help address the challenge of taking our organizations to the future while the other traditional units can prepare for wars based on the previous paradigm; [180] and (3) they can be models to motivate all the other units in the organization. In addition, automation is a unique ability and we therefore need to create divisions that specialize in AI.

One type of new unit should be based on collaboration between humans and robotics. In 2050, army field divisions will be based on robotics, but it is unrealistic to achieve this vision within the next few years. Therefore we need to choose a few small, special units and build them toward the vision for 2050. These new units will help fulfill part of the missions during the next few years, envision the future, and develop a long-term plan to realize this vision.

Creating Data Analyst Positions and Professional Data Sections

Each national security body must have a specific department whose activity is data. This unit will help connect the data tasks both within the organization and among the other organizations. Such a department will be responsible for continuously organizing the data in the relevant context, bringing more data into the organization, and being connected to the databases of other organizations. In the coming years, every organization that wants to survive and to succeed in its digital transformation must build

its own specific department to deal with the foundations of data.

Another trend that is developing, and for which the information field should assume responsibility, is the professionalization of information. Every basic intelligence division (section, small department, etc.) needs to have its own data analyst officer; such a position will require an individual to have expertise in the various databases and to serve as the organization's information expert.

Creating Data Mining Analyst Positions and Data Mining Sections

Another unit is the one that specializes in the use of information (mining and manipulating data). While each officer or operative must know how to probe the data by him- or herself, experts are also needed who are able to investigate various databases and who specialize in constructing complex queries. The information-mining intelligence officers need to have one foot in with the technological specialists of data science and the other foot in with the intelligence analysts in all the units in order to facilitate deep collaboration.

Building Expertise for New Sensors

Additionally, intelligence units involve sensors and specific sources. In the DE, all sensors are an integral part of the information explosion. There seems to be no need for task-specific sensors because each one creates items of information that are supposed to be part of the information endeavor. Nevertheless, task-specific sensors are relevant, particularly those that "dwell" in a particular location and are able to collect and compile information that is found there. Without these types of sensors, this information would be lost. Usually, the purpose of the sensors is the opposite of those designed to create accessibility; these are designed to

ensure that existing information is not wasted. Furthermore, specific sensors play a unique role in the transformation of the organization. A sensor gives a tangible view of a new capability in a location, thereby creating energy in connection to its establishment. Deploying specific sensors is important when it comes to exporting the Digital Revolution, because when sensors are deployed, one must insist on an enabling architecture. This means that all of the sensors are connected to the information tasks (in real time), and fused with the other components of the information.

4. "Accelerate the Acceleration"

The key point is that every organization, every unit, and every department should choose issues that can be accelerated by AI and just do it – which means building units that can lead this acceleration and create new job positions to achieve it. The whole notion of acceleration can yield enormous success.

Leading a Revolution in the Possibility to Produce "Targets in Context"

As we discussed, synergetic learning between human intelligence and AI has the ability to produce tens of thousands of targets before a war and also produce thousands of new targets every day during the war. In addition, the ability to create "targets in context" means that the military can attack the right targets at the right time. This new opportunity enables us to create many more more targets than before and to change the battlefield. [181] Therefore, in order to realize this idea, we should create new units to produce targets based on big data.

Automation for Intelligence Processes

One of the first questions that should be asked in order to lead the AI Revolution is what are the actions, processes, and capabilities that we can automate. AI enables the building of automated machines that perform and represent parts of human cognition; hence, one of the main innovations of AI is automation. For example, China and Russia decided to automate 20-30% of their military equipment by 2025. The era in which human intelligence and artificial intelligence are merging enables automation of intelligence processes traditionally done by analysts. Every organization must ask itself what are the actions, processes, and capabilities that can be automated by using AI. After that, they must formulate concrete plans to improve these automations every month, and to achieve bigger advantages every year. The first new opportunity is to automate intelligence processes in a way that can create new abilities that were not possible beforehand. Under this umbrella are new opportunities to do the same things – only faster and on a larger scale. [182]

Positions and Functions That Can Be Replaced by AI

Over the next few years there will be at least a few positions and functions that could be replaced by AI machines, and we can imagine a distant future in which different kinds of functions and jobs will be replaced by the machines. In the near future, it will be our generation's responsibility to discover these initial positions and functions that can be replaced by the machines.

Automation for Tasks of Audio-Lingual Analysts and Image Analysts

Today, intelligence establishments have thousands of audio-lingual, image, and video analysts. The idea of Speech-to-Text (STT) and machine-learning for images and analysts creates the potential that within five years, more

than 80% of these tasks can be replaced by AI machines.

AI Machines for Cross-Checking Data

For years, intelligence analysts have been working hard to cross-check data. "Is it cross-checked information?" is a familiar question for every intelligence officer. Data with one indication does not have the same credibility as cross-checked data. Over the last few decades, one of the exams for intelligence analysts is to successfully cross-check various pieces of data; this means finding different pieces of data that support each other. Machine-learning has the ability to cross-check the different types, but more than 50% of this function can be replaced by AI machines within just a few years.

Accelerate Narrow Automations for Specific Robotics

Automation covers a wide spectrum: On the one hand, no automation at all, and on the other, full automation. Accelerating the process of automation requires narrowing the capabilities chosen to be replaced by automation and beginning with these choices. [183] Robotics also comes from the family of automation. Our weapons and vehicles have the potential for automation over the next 20 years. From the perspective of 2020-2025, we need to choose specifically which of these can be replaced and improved by robotics. [184] The first part of this mission is to build a concrete, narrowly focused plan. Drones are a great example. [185]

Drones have a new potential to acquire tremendous image knowledge. Drones with AI capabilities can control a specific geographic location and accelerate the potential to collect details as well as analyze the relevant information. Moreover, the potential to build a swarm that includes hundreds of drones with AI capabilities is a vision that can be realized in

two to three years and can be a game changer for our missions. The great potential for drones is the reason that China made their interesting decision to build AI-capable drones and to build them with the ability to act together in a swarm of more than 1,000.[186] Reaching their potential – to be a player in national security – requires the development of a "drones division."

5. FAST for Enabling MDO (Multi-Domain Operation)

Over the last several years there has been a discussion in the U.S. military about moving from the concept of Multi-Domain Battle to Multi-Domain Operation (MDO). This means merging different capabilities and different domains (air, sea, ground, cyber, information, and space) to a joint operation. During the fourth Industrial Revolution, changes and incredible innovations occur at a rapid pace, one after another. These advances are built "on the back" of the previous innovations. In addition, there are collaborations between innovations that create new capabilities. However, it is difficult to merge different types of innovations. The data is infinite and expands every moment, there are ever-increasing new technologies, and every day there are new capabilities. Therefore, it is complicated to join and merge all of these new technologies together.

From a military perspective, the Navy can collaborate with the Air Force, but it is very difficult to merge all of the forces into MDO. Every organization has its own big data, and it is difficult to have them act together. Traditionally, there have been collaborations on missions, and in the last few years there have been multi-domain battles. However, this is collaboration and joint forces for a specific battle, and not for Multi-Domain Operation. Although this will be one of the missions in the coming years, there are challenges to realize the concept. For example, can a common operating picture of all the domains be created? Another

challenge is that each domain works on a different timeline. To realize the idea of MDO, the military needs the ability to merge the various domains' abilities into a common operating system on the same timeline, as well as to build foundations that can support this new concept. [187]

How and Why the Idea of The Human-Machine Team and the Concept of FAST Can Realize the Plan for MDO

The first reason is the new potential from data and intelligence. The domains are different, but if the "playground" is based on common foundations, all domains can operate together. Traditionally, data and intelligence have been a "support effort." For years, the function of the intelligence establishments for the military has been to be a support effort, similar to the logistic effort. There are main efforts and there are support efforts, and the information that the intelligence analysts are required to provide is one of the support efforts. However, as we discussed, in the Information Age the data is not only "to support," it is the basis for almost everything. Data is the basis to create targets, to attack these targets, and to find the enemy. It is also the basis to understand when, where, and how both friendly and unfriendly forces are active on the battlefield. A lot of the data is classified, and the unclassified data is also more relevant when it merges with the classified. Therefore, intelligence organizations are responsible for organizing the data for all the military organizations and for making sure that the data designs the playing field for everyone. When the foundations include a common "data center" and the ability for every domain to use it, there is potential for building a Multi-Domain Operation.

Common or mutual foundations means: 1) keeping and tagging all the big data with cloud technology; 2) having a closed-open-closed network to address the classified and unclassified data in the same system and on the same network; and 3) strong power-computing to use all this data. The

foundations do not have to be same, but they must be mutual for all domains, with connections among the domains and similar architecture. An example is an air force cloud that can connect and pass data from the navy cloud, or a cyber network that can use data from the ground forces network.

The second reason that the idea of The Human-Machine Team and the concept of FAST can realize the plan for MDO is the new potential for "joint acceleration." This means building small, multi-domain units based on collaboration between the capabilities of fighters from different domains with robotics and AI automation. It includes the automation of military hardware such as weapons, vehicles, and drones, and the automation of analysts' functions, etc. These types of units have the potential to be growth engines to lead the concept of MDO.

The third reason is that The Human-Machine Team and FAST create a new potential for merging different timelines and pictures due to the collaboration between human and artificial intelligence. For example, over the last few years, the IDF (Israel Defense Forces) has developed a new concept of Intelligence Centric Warfare to connect intelligence to the fighters in the field. [188] This revolution follows the changes in the DE. One of the goals of intelligence-centric warfare is to expose the enemy and make intelligence accessible to the soldiers at every level and in every location. The concept of The Human-Machine Team will be the next generation of the merging of intelligence and warfare, which can be a new potential of collaboration between different domains. In other words, when data, innovations, and fighters can merge into one vector, there is the potential to realize the vision of MDO. [189]

---

173 Yuval Noah Harari, op. cit., 73-81.
174 Ajay Agrawal, Joshua Gans and Avi Goldfarb, op. cit., 43-48.
175 Executive Office of the President National Science and Technology Council Committee on Technology, op. cit., 15-16.

176 Henry Etzkowitz, Chunyan Zhou, *The Triple Helix* (city? Routledge: 2018), 21-37.
177 Congressional Research Service, op. cit., 13-16.
178 2018 DoD Artificial Intelligence Strategy, op. cit., 7-8.
179 Preparedness means protecting your homeland against a surprise attack, or being ready to send your forces on an emergency mission without much time to train.
180 Chapter 5: Challenges and Difficulties.
181 Chapter 3: Deep Defense.
182 Ajay Agrawal, Joshua Gans and Avi Goldfarb, op. cit., 114-117.
183 Stuart J. Russell, Peter Norving, op. cit., 988-990.
184 Ajay Agrawal, Joshua Gans and Avi Goldfarb, op. cit., 114-117.
185 Congressional Research Service, op. cit., 11-13.
186 Ajay Agrawal, Joshua Gans and Avi Goldfarb, op. cit., 164.
187 Hawk Carlisle, National Defense, "The Complexity of Multi-Domain Operations." November 28, 2017. http://www.nationaldefensemagazine.org/articles/2017/11/28 /the-complexity-of-multi-domain-operations
188 Intelligence-Centric Warfare. In the past, it may have been enough to provide the tactical level with the general position of enemy units in a given area and their basic combat doctrine. However today, when the enemy is hiding and constantly disappearing, a general description of the location and nature of the forces is no longer enough. This means that intelligence priorities and focus will have to change to support the intelligence needs at the tactical levels. A profound technological, organizational, and cultural change will be necessary for this to occur. Aviv Kochavi, Eran Ortal, "Ma'asei Aman": Permanent Change in a Changing Reality." (*Cyber Challenges and Opportunities in New Realms, the Dado Center Journal,* December 2014, pp. 20-30.)
189 On the "Revolutionary Impact on Combat," see Congressional Research Service on *"Artificial Intelligence and National Security,"* (April, 2018), 36-38.

CHAPTER 9

4 x 4: A Powerful Management Tool and the Required Leadership

"4 x 4" (4 years, 4 months, 4 weeks, and 4 days) is shorthand for a great management method to lead digital transformation. Specifically, 4 x 4 is a relevant method for leading nations and organizations to the future era of The Human-Machine Team. In my professional experience, we implemented 4 x 4, and it appears to be a winning method. The size and complexity of the AI Revolution also poses a challenge to the management approach that will be used. Traditionally, leaders and managers used to say, "I will tell you what to do, and you will tell me how you are going to do it." The teaming of humans and machines, combined with the fast pace of innovations, has changed the order. This means, as we discussed, that the "how" defines the "what" more than the "what" defines the "how." Therefore, a method of how to lead nations and organizations to fulfill the plan is more important than the plan itself. One of the concerns is that we will dream too big and be left only with dreams and presentations without real transformation. There is also the fear that in order to be sufficiently practical, we will carry out measures that are too small and too local, that will not bring about a wide-scale revolution. Thus we arrive at the management tool in 4 years, 4 months, 4 weeks, and 4 days to organize the complex, dynamic nature of our missions.

It is extremely important and takes courage to dream that we have the ability to change both the security concept and a way to implement the change. The DE provides a tremendous potential for massive revolutions. Therefore, a practical tool is required to build the road, step-by-step, to fulfill the dream. The 4 x 4 tool requires us to begin the process,

accomplishing the mission by (1) summing up the concrete steps we can and must take within the next 4 days; (2) identifying what information, its organization, composition, etc., can be advanced in the next 4 weeks; (3) deciding which measures we must and can advance in a time frame of 4 months; and finally (4) agreeing on our goals for the next 4 years.

The unique and dynamic nature of the 4 x 4 tool matches the dynamic nature of the mission because these 4 different aspects are reviewed every week, at the end of which we re-examine all the stages: what we completed in the previous 4 days and what we need to do in the next 4 days; how we should progress on the tasks that were set for the next 4 weeks; and what is the updated status of the outputs we are committed to complete in the next 4 months. The end of this weekly 4 x 4 is a review of what we learned, as well as an update of our goals for the next 4 years. Imagine the power this tool has – to incrementally accomplish a difficult, complex mission. The pace of change in the DE requires this type of management tool.

Moreover, in an era in which the amount of data increases every moment, the best way to learn and carry out revolutions is through friction. The 4 x 4 method makes it both possible and necessary to encounter friction all the way to the big revolution. Furthermore, this method allows one to celebrate the small successes during the journey – the kind that give strength to continue the challenging work. One cannot tarry too long at the dreaming stage; the operational outputs have to be shown very quickly, through intelligence and operational practice. Thus, already in the beginning stages, there is a need to select significant issues that can be addressed differently, with the capabilities developed as part of digital transformation. These successes will generate the energy (internal and external) to continue the challenging work. The system to lead this revolution is the innovation ecosystem. [190]

Required Leadership

Defense leadership in the DE is changing. Leaders today need to lead their nations and organizations to digital transformation. They need to address new challenges that are developing as a result of DE. Defense leaders are required to deal with structural and cultural challenges to digital transformation; in addition, they must use the new potential of The Human-Machine Team to understand, influence, and empower life experience, and to mitigate risks and take advantage of opportunities by using digital bits. Leaders have the responsibility to solve, or at least confront, problems that human beings did not know how to solve in the past. Digital transformation requires a substantial investment of time – specifically, managers' time. A realistic estimate is that no less than 40% of a manager's time should focus on digital transformation. [191]

Leaders also need to formulate strategy on how to deal with rivals and enemies who are also in the middle of their Digital Revolutions. Security leaders need intelligence about the digital transformation of their enemies and rivals as a basis for their strategy on how to act against them. They also need to ask themselves how they can influence the transformations that their rivals and enemies are going through due to the Digital Revolution. It is not your imagination that you can influence your enemies' and rivals' DE Revolution.

Leadership is based on the competition of learning. Security leaders deal with enemies and rivals who are changing all the time, which is why the leaders are required to be constantly learning. The difference between a mediocre and great leader is the ability to impact big issues based on this process of constant learning. The struggle between hostile states, and between leaders, is not only a "power struggle;" victory is not based only on superior aircraft, tanks, or financial resources. Victory, and the ability to be

a successful strategic leader, is also based on winning the learning competition. The strategic leader who studies all the time will be the leader who wins the competition. He will be the one who is best able to face complex challenges. The leaders who guide their nations and organizations to win the AI competition will be the ones who shape the future and will, in fact, "control" it. Defense organizations that lag behind in the AI Revolution and do not succeed in transforming themselves towards the concept of The Human-Machine Team will fall behind and lose the competition.

As we discussed, the AI Revolution is a new, high-level paradigm. During the transition period between paradigms, the previous paradigm will always try to hang on and beat the new high-level one. Since we are just at the cusp of this revolution, the previous paradigm is still relevant; however, the future belongs to leaders and organizations that will restructure themselves toward the concept of The Human-Machine Team. For the foreseeable future, security leaders need to hold on to the previous paradigm, and at the same time reach for the new one. *There is no choice* . Security leaders are required to transform their organizations for the future of AI while maintaining the traditional capabilities at the same time. Organizations that succeed in combining The Human-Machine Team and the capabilities of the previous paradigm will have the potential to win during the transition period.

The first and most critical factor is understanding the importance of creating a strategy for the DE. Leaders must formulate a vision for their organizations for the DE; they must have basic knowledge about digital, cyber, and AI. They also need to have the ability to explain their digital system. They cannot just say, "Digital is important" and have someone else explain the strategic vision for digital transformation in their organizations; they must have basic knowledge and the ability to do it by themselves.

Artificial intelligence is a new concept that is relevant for all fields and for various subjects; therefore, we need AI education to enable more and more AI scientists and analysts. Moreover, we need education for leaders and managers. In our generation, they are required to have the ability to lead their nations and organizations to the era in which human and artificial intelligence are merging. In addition, in order to develop the relevant knowledge, they need to understand the current status of the AI of their rivals and enemies. For example, due to the situation today (how China and Russia view AI), we need to acquire a profound understanding about AI in those countries (strategy, plans, people, etc.). Therefore, one of the first places to deal with AI and to educate AI analysts is in governmental research divisions.

One of the ways to think about the future is the concept of scenarios. Keens Van der Heijden, in his book *Scenarios: The Art of Strategic Conversation,* develops scenarios as alternative ways to make sense of what is happening in the environment, and using them to become more secure about the future. He also discusses how to do all of this as an organizational process to impact the thinking of the organization as a whole and prepare it for action. Van der Heijden explains:

> "…strategy is about winning in this process…strategy is a highly dynamic area, full of fads and fashions that come and go…success can only be based on being different from (existing or potential) competitors…today's best strategy may be tomorrow's disaster… the practice of scenarios-based planning process… we will base this discussion on the premise that the ultimate purpose of the scenario planner is to create a more adaptable organization, which first recognizes change and more uncertainty, and second uses it creatively to its advantage". [192]

Security leaders are required to build scenarios for the security challenges due to the DE Revolution. They should practice scenarios of risks and opportunities as a result of the concept of The Human-Machine Team. These leaders must formulate scenarios for the AI Revolution as a basis for their planning processes.

The Culture of Sharing and Culture of Entrepreneurship

"Culture eats strategy for breakfast." [193] It is very difficult to change a culture, and it takes years to accomplish. However, when you want to be in a process of changing, your culture needs to support the change. The DE Revolution is a new, high-level paradigm. The Human-Machine Team is a novel concept of thinking and acting together. Therefore, for an organization to succeed in leading transformation, it is also necessary to examine the need for cultural changes.

Sharing

First, let's examine how a culture of sharing aids transformation. In the DE, people are used to sharing with each other all of the time. For example, if you see something interesting, the first thing you do is take a picture of it and share it with friends and family. If you have new information, or new knowledge, you share it through social media, the internet, or some other way. AI builds on data and experiences, and the more data and experiences, and the more variety, the better. Therefore, departments, units, and organizations that participate with other organizations or sections have greater potential to build their Human-Machine Team.

Normally, national organizations share information up and down to the managers and back to the employees, but not sideways to the full breadth of the organization. Security organizations typically relate to their

information and their knowledge as power and as classified, and they try to share the least amount required. However, to build a merger between human intelligence and artificial intelligence, organizations must also become comfortable with the culture of sharing. Organizations should build their information infrastructure in a simple way to share information both within and outside the organization. This culture will create better conditions to realize the transformation and take the organizations to the future. In addition, national security organizations need to create AI networks among all the agencies and to share ways and efforts to fulfill the concept of The Human-Machine Team.

In other words: The world belongs to those who share. People have always sought to connect information with information. For example, in the margins of the pages of the Jewish Codes of Law (the Talmud), the reader is offered references that connect the text on the page with other texts in the Talmud as well as with other related texts from additional Jewish sources. These links constitute knowledge in itself. The internet era has developed, refined, and expanded on this approach. The ability to wander among the pages of the internet and connect between one item of information and another has enhanced the understanding that the "links" constitute knowledge in and of themselves.

In the DE, collaboration in information, knowledge, and operative activity based on data constitutes a condition for success. The deeper the collaboration, the greater the ability to provide a better intelligence response. When it comes to information and knowledge, the challenge of collaboration is, unfortunately, not simple. Many people and organizations believe they must safeguard the information they have solely for their own or for their organization's benefit. In the DE, the world belongs to those who manage to overcome the challenge of collaboration, to those who share with others, and with whom the others share. One must understand

the critical need and invest in the critical ability to share information back and forth. This is first and foremost a systemic-conceptual challenge, but it also entails a complexity of architecture that enables the sharing of information. The consent of different organizations is required, as is an architecture that makes it possible to implement the agreements regarding sharing information in a simple fashion. However, it is understandable that both aspects are complex and daunting.

More Women in High-level Positions

Today our reality is still one in which most high-level positions are held by men. In security establishments, the reality is more extreme. The ratio between men and women in such positions differs among countries and organizations; nevertheless, in all countries, most security and military leaders are men. Female leadership and management naturally bring more of a culture of sharing. Women usually possess more of a style and culture of managing together with a bit less competition. Security establishments need to increase the percentage of women in senior management and leadership roles; the target should be 51% women. Nations and organizations that increase their percentage of women leaders will be more relevant in the DE and better able to realize the concept of The Human-Machine Team. [194]

Internal Entrepreneurship and Trusting Your People

National security organizations typically have a culture organized by hierarchy and a culture of testing output. To lead these organizations into the future, their leaders and managers should support the internal culture of entrepreneurship. For example, they can implement concepts such as "a week out of the box," in which a group of people is taken out of their usual

units and missions and tasked for a short time to create ideas for the next AI innovations. In addition, it is important to have internal startups in the national security establishments that focus on AI. This means supporting small groups within the organization that function like internal entrepreneurs (given the freedom and the resources to develop new ideas for taking advantage of AI).

Trust and believe in your people, and know that they know what they can and need to do. Use the hierarchy as little as you can, and give them as much space as possible. In addition, keep your organization in near-chaos. This does not mean that all organizations are required to be in such a state, without any organizational hierarchy, and with the trust that their people know what they need to do. It depends on your expectations for your organization. When you know the end state, and you just want to improve productivity, you can use the tools that have been developed during the Industrial Revolution, and build your organization like a machine. When you want a culture of innovation, when you want to build new capabilities and be in the process of changing, give up the requirement to be in control and give your people the space to act in their own ways.

An interesting example of this is the Future Command that the U.S. Army established. The unit's purpose is to lead its organization to reach future capabilities and then share the advances with all divisions of the Army. The culture in the Future Command is not like that in normal Army divisions, with interaction based on traditional hierarchical organization and seeking to function like a machine. When you want to lead these types of innovations, you must use hierarchy as little as possible and give your people as much space and flexibility as you can. This is why it is so important to build unique departments or units that focus on innovation, and to make sure that a different culture will be a main characteristic inside these units. It is common to imagine cultures of organizations with different

metaphors. [195] During the Industrial Revolution, many organizations were built like machines – to improve productivity in the organization. A main metaphor for organizations in the DE should be "flux and transformation" [196] – flux as one of the main drivers to take the organization successfully into the future, and transformation to successfully realize the new dreams.

---

190 Col. Y, op. cit., 21-22.
191 Stuart J. Russell, Peter Norving, op. cit., 437.
192 Heijden, Keens Van der, *Scenarios: The Art of Strategic Conversation* (publisher? West Sussex: 2010, preface).
193 It is a famous idea coined by Peter Ferdinand Drucker, an Austrian-born American management consultant, educator, and author, whose writings contributed to the philosophical and practical foundations of the modern business corporation . He has been described as "the founder of modern management". Just write "See end note #155.
194 Thomas W. Malone. op. cit., 35-37.
195 Morgan Gareth, *Images of Organization* (city? SAGE: 2006). Chapter 5.
196 Morgan Gareth, ibid., Chapter 8.

EPILOGUE AND PERSONAL NOTES

"Too good to be true." This is the answer that I gave thousands of times when I was asked how my year in Washington, D.C. was going. I had arrived with a few goals, but couldn't have imagined that this year would change my life and be a kind of tipping point for the rest of it. The first mission for the year was to improve my English. After two weeks I decided that my American Dream was to work to make my English as good as my Hebrew. I knew that it was unrealistic, but in the U.S., everyone has his or her own American Dream, and a main pillar of American culture is that you can achieve your dreams if you work hard enough. To try to make this dream a reality, I shifted all of my life to English. I bought a laptop without Hebrew characters, changed the settings in my smartphone to English, and started to talk with my wife and my Israeli friends in English. I still have a long way to go. This book began as part of the dream, but after a few weeks the book took on a life of its own.

The National Defense University is really an amazing place that gives one the ability and the facilities to learn and build a global network. We were 70 international students from 54 countries; there were also a few hundred American students (from the military, government, and private sectors). The concept of how we studied together helped build strong relationships, and it is clear that this networking process will be used throughout our lives. Moreover, the international students' program is, in one word: amazing! It consisted of an excellent team, a fascinating program, and educational trips all over the US.

The biggest change that "just happened" to me during this year is a new framework to look at Israel as part of the world. Throughout my life, I often found myself thinking about Israel – what we need to change, the challenges we face, and how we can overcome the challenges. For the first

time, during the year at the NDU, I began to think about Israel as part of the world – which it is a really dramatic change for me.

The process of writing this book was an exciting journey. I began it without understanding the end state. I also began the journey knowing that it could lead to a dead end. The process required examining basic assumptions, renouncing old paradigms, and adopting new ones. It opened doors that did not previously exist and enabled dreaming of new things. A few times, I felt like someone who embarked on a new route, sometimes got wounded, and even lost blood (because the route is unpaved and full of thorns), and sometimes comes to a precipice, or a dead end, and has to go all the way back. Thankfully, during the difficult times, the end result usually involved exciting breakthroughs that paved the way for new paths.

During my exciting journey, I found myself talking about AI and about the idea of The Human-Machine Team every day, with different people, and in different places. These discussions greatly helped me organize my thoughts, change my concepts, and to coin my words. I need to thank hundreds of people – friends, colleagues, family, and many others. I need to apologize to the people who met me for different reasons and I talked to them only about AI. My eldest daughter, nine years old at the time, used to say to me during this journey, "Daddy, I must tell you AI is not so interesting and is not the most important thing in our lives."

The future is already here, but it is not divided equally.[197] This means that usually the big things that we will see over the next few years are already here, but just in specific areas and not as part of the mainstream. In the future, these unique things will be part of our everyday lives, and new inventions will be unique. After a few more years, the next one-of-a-kind invention will become the mainstream and so on. This book has attempted to take our nations and organizations years ahead. Many of the ideas that we talked about are already here, and we "just" need to take them from the

periphery and deliver them to the center of the stage and to the center of organizations.

The "clash of civilizations" is a famous theory created by Samuel Huntington . He claimed that people's cultural and religious identities will be the primary source of conflict, and that future wars will be fought between cultures, and not between countries. According to Huntington, "This is not to advocate the desirability of conflicts between civilizations. It is to set forth a descriptive hypothesis as to what the future may be like." In addition, the clash of civilizations, for him, represents a development of history. In the past, world history was mainly about the struggles between monarchs, nations, and ideologies, such as seen within Western civilization. However, after the end of the Cold War , world politics moved into a new phase, in which non-Western civilizations are no longer the exploited recipients of Western civilization, but rather have become additional actors joining the West to shape and move world history. The Digital Era is a historic perspective to describe our own era, when a big revolution is taking place. The Human-Machine Team seeks to deal with the new challenge when the Clash of Civilizations meets the Digital Era and creates "data civilizations." On the one hand, "the world is flat" and everyone can communicate with everyone else 24/7, and all over the world; on the other hand, the world is *not* flat, and every civilization lives in its own "data civilization." [198]

The Human-Machine Team is just part of the beginning of the journey that nations and organizations must make in order to acquire the new potentials that the era of AI is bringing. Using the terminology of Thomas Kuhn's book (mentioned in the Preface), *The Structure of Scientific Revolutions* , we are a transition generation, which entails confronting numerous and complex challenges. The competition between enemies and rivals is a competition of learning. It seems to me that in the next few years,

the learning competition will take place primarily in the field in which *human intelligence and artificial intelligence are merging* . Nations, organizations, and companies that build the best Human-Machine Team – based on the concept of FAST – will have a huge advantage in the future that is already the present.

The End

Or, in fact, just the beginning of the future .

---

197 It is a paraphrase of William Gibson's idea "The future is already here – it's just not evenly distributed." Gibson is known for coining the term "cyberspace ."

198 Yuval Noah Harari, op. cit., xv, 100-102.

ACKNOWLEDGMENTS

This book is a journey I took with friends, colleagues, professors, commanders, family, and many others, as well as a journey through organizations in Israel and the U.S. All the ideas in the book are the products of this common journey. Everything is the fruit of hard work, ongoing discussions, and joint creation. The most important ideas were born in the wake of disagreement with those who thought otherwise. It is a pleasant obligation to thank everyone. The mistakes are my responsibility. The innovations here come from true partnership. I would like to personally thank all those who worked long, hard hours on the book, providing ideas and proofreading; the book could not have been written without their help.

I would like to thank my teacher, my friend, and my "havruta," Seth Riebman. Seth started as my English teacher and became an integral part of this journey. He helped me shape the ideas, correct mistakes, and realize my dream.

It is a great privilege for me to thank the National Defense University, which became a part of me during my amazing year in the U.S. The NDU has a culture of learning and is an institute that trains leaders from all over the world – leaders of the present and the future. I would also like to thank the Eisenhower School and the great team of educators at that astonishing place. A special thanks go to the professors who were also my advisors during this journey: Dr. James Keagle, who also gave me the idea for the name of this book and supported me and pushed me all the way; Capt. Frank Futcher, who lead our seminar about AI and helped me hone my thoughts; and Dr. Steve Brent, who connected this issue to the economy and to industry. I also thank Dr. Frank Cooling – who pushed me

to take this journey – for his intelligent suggestions, and Dr. Seth Weissman, my personal advisor during the year, for all his great support. Personal thanks also go to Dr. T.X. Hammes, for his pointed remarks, and to all my other professors and colleagues. Special thanks go to Jorge Ascunce and the staff of the International Student Management Office. The year is thanks to all of you, and I will never forget it. I would also like to personally thank Mickey Edelstein and Michal Duvdevany, and everyone else at the Israel Defense Forces Attaché's Office in Washington, D.C., who helped me get to Washington.

I must also thank my mentors and friends from Israel who accompanied me: Dr. Amos Granit, who helped me build the framework for this journey and didn't spare me any difficult questions, and Dr. Hadas Minka, who helped me begin the journey and make the right decisions along the way. Special thanks also to Gur Amibar and David Karpf, who both provided me with personalized proofreading during my writing process. I am also grateful to my colleague, partner, and fellow student during the year at the NDU, Shlomi Binder, with whom I first discussed the ideas in this book, and who helped me fix up the manuscript. Additional thanks to Abby Peleg and Debbie Hemi, my English teachers in Israel: you both gave me the ability to set forth with my dream.

The journey could not have been completed without Dr. Shay Hershkovitz and Nadav Zafrir, the co-founder of "Team 8" and a former commander of Unit 8200, the "Israeli NSA" (2009-2013), who both helped me re-organize my manuscript to become a book. Nadav and Shay: you both gave me a big gift, and this book belongs to you, too.

A huge thanks to the NDU Press, and specifically to Bill Eliason, director of the NDU Press, and to Mr. Jeff Smotherman, who both demonstrated professionalism and made me feel that the NDU Press is my home. You demanded a lot of changes and helped me improve the manuscript. Today,

when I look back at the first draft, I can't believe the huge changes you helped me with. This book is definitely thanks to you. Working with you was a great honor, and I look forward to collaborating in the future. NDU teachers Katy Denman and May Chung, who helped me improve my writing so much, word by word, and page by page, also deserve my deepest gratitude. My thanks to Ebookpro and Kim Ben Porat – with your help I succeeded in completing this journey.

For the last 20 years, the Israel Defense Forces (IDF) has been my second home; it is also part of my identity. The men and the women of the IDF are more than amazing; they have great souls and are full of care and motivation. Most of my experience has been in Israel Defense Intelligence (IDI), and I feel great pride in being a part of this organization. I would like to thank my commanders, my colleagues, my subordinates, and my friends in the IDF. This journey to The Human-Machine Team is both thanks to you and for you.

A personal thanks to my parents and siblings for helping me build my identity. A final, and the most important, expression of gratitude is for my wife, Tal, and my children, Hallel, Itamar, Yonatan, and Alma. All that I have done is thanks to you, and the journey belongs to you.

I hope that this journey will be an additional brick in the strengthening of Israel, and for the security of the free world, and and that it will help lead the world to becoming a better place for all humankind.

Hallelujah. Hallelujah.

LITERATURE REVIEW

Less is More, and Clarity is Power

Yuval Noah Harari begam his book 21 Lessons for the 21st Century with an astonishing sentence: "In a world deluged by irrelevant information, clarity is power." My professor and advisor at the National Defense University, Dr. Jim Keagle, says that "In our days, less is more." These two concepts were right in front of my eyes when I decided how to describe the literature review for this book.

One of the big revolutions in the DE is the ability to communicate – instantaneously – with all of the people all over the world. This revolution has created the reality that took us from the days when we didn't have enough data, to the current reality of an infinite amount of data. During my career, the complicated challenge was to acquire more and more data. Today the challenge is to discover the relevant data that is in the infinite stack – something even more difficult than finding a needle in a haystack. This is the background and the reason for the development of "data science."

Therefore, I decided that the literature review will be part of our journey to achieve clarity and to keep this amazing and complicated process as simple as we can. Like this book, this chapter is intended for various types of people: scientists who want to understand the big picture about AI and the collaboration between a human and a machine; every woman or man who wants to understand why and how AI is changing the world; managers who want their organizations to address the current Digital Revolution; and national security leaders who want to lead their establishments to the era in which human and artificial intelligence are merging.

The Structure and Limits of This Review

I have tried to organize the literature review in a way that helps understand our journey and find the relevant references. In addition, I would like to enable you to use this review for your own journey. As we discussed in the book, artificial intelligence has the potential to be a game changer and to address big challenges in new and different ways that years ago we couldn't have even imagined. It can potentially improve healthcare, national security, personal security, and many more critical areas of our lives. A world with artificial intelligence is a new world; for that reason, we hope that this review will be an easy starting point for more and more journeys to a future that has already become the present.

I have tried to be as concise as possible. There are many books, articles, and websites, and I have tried to provide the key ones that helped me write this book. From my point of view, they are all basic, yet critical references. Finally, the most important and influential input for this book came from discussions with amazing people – friends, colleagues, professors, advisors, and many others that I met during this journey.

Inspirational Literature

Many of the books that I found along my journey discussed the future 20 years ahead, or even more. Now, in the "Spring of AI," innovations and concepts are changing even as you read this; therefore, books that are about the distant future are more for inspiration than for specific steps. These books served as inspiration, and helped create my vision of how to transform national security in the era of artificial intelligence.

Ray Kurzweil helped me make the decision to begin the journey. His book, "The Singularity Is Near" was one of the reasons I decided to become a part of this revolution.

Kurzweil, Ray, "The Age of Spiritual Machines" (Penguin Books: 1999)
Kurzweil, Ray, "The Singularity Is Near: When Humans Transcend Biology" (Penguin Books: 2005)
Yuval Noah Harari facilitated my taking complicated issues and expressing them in clear concepts and words. He also helped me discover how the digital era is going to have an influence on various fields all over the world, and in all our lives.
Harari, Yuval Noah 21 Lessons for the 21st Century (Spiegel & Grau: 2018).
Thomas L. Friedman was my inspiration for creating the big picture. In addition, he inspired me to try to write about the complicated issues in language that will be relevant and interesting – not only for national security leaders and scientists, but for anyone who wants to learn about this complicated subject.
Friedman, Thomas L, *The World is Flat: A Brief History of the Twenty- first Century* (Picador, Farrar Status and Giroux: 2005).
Friedman, Thomas L, *Thank You for Being Late: An Optimist's Guide to Thriving in the Age of Accelerations* (Picador, Farrar, Straus and Giroux: 2016).

AI As a Cause for a New Strategy

The basic concepts of strategy were formed during the Industrial Revolution and with the characteristics of the revolution. What is strategy in the digital era? Who is the strategic leader that knows how to take his organization or his country to the future of the digital era? To provide our strategy framework, I relied on two popular books about strategy. The first, *Strategy Safari* was a refence for the basic ideas about strategy and a reference for asking "What is changing?"
Mintzberg Henry, and Ahlstrand, Bruce, and Lampel Joseph, *Strategy Safari: A Guided Tour through the Wilds of Strategic Management* (Simon &

Schuster, 2010).

The other was Van der Heijden's book on scenarios. He develops scenarios as alternative ways to make sense of what is happening in the environment and to use them for a more secure future. He also explains that "…**today's best strategy may be tomorrow's disaster** …the ultimate purpose of the scenario planner is to create a more adaptable organization, which first recognizes change and more uncertainty, and second uses it creatively to its advantage." [199] This concept helped build an alternative near future for national security establishments when AI and humans merge.

Van der Heijden, Keens. *Scenarios: The Art of Strategic Conversation* (West Sussex: 2010)

"The Bible of Artificial Intelligence "

Russell, Stuart J, and Norving, Peter, *"Artificial Intelligence: A Modern Approach* " (Pearson: 2015).

The first time that I came across this book was when I read an article that was put out by the Executive Office of the President, which describes the book as popular and basic. I call it "The Bible of AI" because it is a remarkable book containing all the basic information about AI, and a book that you can learn from, from beginning to end. You can go back and forth to every chapter and continuously use it as a source of knowledge. During my journey, it never left my desk, and every time I opened it, I learned something new. Granted, it is long (1,145 pages!), but it is easy to find the relevant issues inside. It is a book to read, to mark, and to write comments and annotations in its margins. Personally, I can't wait for its fourth edition to be published.

Basic Research Papers

During my journey, I read hundreds of papers. A few of them were the most relevant and influential and include basic definitions and basic knowledge. They help give the answers to "What has changed?" that enables us to realize the 70-year-old idea of AI. The papers also include relevant recommendations from the big picture of a national perspective.

- Executive Office of the President. National Science and Technology Council Committee on Technology. "*Preparing for the Future of Artificial Intelligence*" (October, 2016).
- Congressional Research Service: "*Artificial Intelligence and National Security*" (April, 2018).
- 2018 DoD Artificial Intelligence Strategy. *Harnessing AI to Advance Our Security and Prosperity* (February, 2019).

Prediction

Prediction is an essential ability of human intelligence. Prediction means learning from information that we have about information that we don't have. *The Human-Machine Team* is, among other things, the ability to create new predictions that we couldn't previously achieve. *Prediction Machines* is a book that helps us understand this complicated issue; moreover, it helps see the process of AI innovations and how they influence our current challenges.
Ajay Agrawal, Joshua Gans and Avi Goldfarb, *Prediction Machines: The Simple Economics of Artificial Intelligence.* (Harvard Business Press, 2018)

Others
Books:

Stone, Deborah. *Policy Paradox: The Art of Political Decision Making* (New

York: W.W. Norton & Company Inc. 2012)
Gareth, Morgan. *Images of Organization* (SAGE: 2006). (Paragraph 8 "Unfolding Logics of Change: Organization as Flux and Transformation."
Scharre, Paul. "*Army of None* " (New York: W.W. Norton & Company, Inc. 2018).
Kurzweil, Ray. *The Singularity Is Near* (New York: Penguin Books. 2005).
Brik, Brynjolfsson, Mcafee, Andrew, *The Second Machine Age* , (New York: W.W Norton & Company, Inc. 2016).
Malone, Thomas W., *Superminds* (New York: Little, Brown and Company. 2018)
Daugherty, Paul R, Wilson, James H, *Human + Machine* (Boston: Harvard Business Review Press. 2018).
Etzkowitz, Henry, Zhou, Chunyan, *The Triple Helix* (New York: Routledge. 2018).
Articles:
Kochavi, Aviv, Ortal, Eran. "Ma'asei Aman: Permanent Change in a Changing Reality" (Cyber Challenges and Opportunities in New Realms. the Dado Center Journal December 2014)
Ryan, Mick. *Human-Machine Teaming for Future Ground Forces* (Center for Strategic and Budgetary Assessments, 2018).
https://csbaonline.org/uploads/documents/Human_Machine_Teaming_FinalFormat.pdf
UK Ministry of Defense. "*Human-Machine Teaming* " (Crown copyright Joint Concept Note 1/18, May 2018).
file:///C:/Users/yossi/Desktop/human_machine_teaming_jcn_1_18.pdf
Intelligence in Theory and in Practice. *Big Data and Intelligence* (a Journal on Intelligence Methodology, October 2018).
Websites:
Friedman, Thomas, " Where did 'We the People' Go?" New York Times,

June 21, 2017, https://www.nytimes.com/2017/06/21/opinion/where-did-we-the-people-go.html
Mintrom, Michael; Norman, Phillipa. " Policy Entrepreneurship and Policy Change" , Policy Studies Journal; November 2009.
"Artificial Intelligence Fuels New Global Arms Race" . *WIRED* . Retrieved December 24, 2017.
https://www.wired.com/story/for-superpowers-artificial-intelligence-fuels-new-global-arms-race/
Paul Mozur. "Beijing Wants A.I. to Be Made in China by 2030", New York Times, July 20, 2017, https://www.nytimes.com/2017/07/20/business/china-artificial-intelligence.html
Gregory C. Allen "Understanding China's AI Strategy", Center For a New American Security, February 6, 2019
https://www.cnas.org/publications/reports/understanding-chinas-ai-strategy
Bendett, Samuel, "In AI, Russia Is Hustling to Catch Up." Defense One, 04 April 2018.
https://www.defenseone.com/ideas/2018/04/russia-races-forward-ai-development/147178/
Bendett, Samuel. "Here's How the Russian Military Is Organizing to Develop AI" in *Defense One* , July 20, 2018.
https://www.defenseone.com/ideas /2018/07/russian-militarys-ai-developmentroadmap/149900/
Wong, Joon Ian, Sonnad, Nikhil. "Google's AI Won the Game Go by Defying Millennia of Basic Human Instinct" March 25, 2016.
https://qz.com/639952/googles-ai-won-the-game-go-by-defying-millennia-of-basic-human-instinct/
Carlisle, Hawk, National Defense "The Complexity of Multi-Domain

Operations" November 28, 2017. http://www.nationaldefensemagazine.org/articles/2017/11/28/the-complexity-of-multi-domain-operations

---

199 Keens Van der Heijden, *Scenarios* : The Art of Strategic Conversation (West Sussex: 2010), pp. xv, xvi.